Cyber Liability

What you need to know!

PRESENTED BY:

• GALLAGHER / CYBER*RISK* SERVICES

MAY 2014

Most Common Reactions to Cyber Liability Questions:

- “We don’t need cyber liability coverage; we have tort immunity protection.”
- “We don’t have the budget to buy cyber coverage.”
- “We’ve got good firewalls; we’re not worried about cyber losses.”
- “We’ll have to wait until something happens; I can’t convince my board to spend the money.”

What is Cyber Risk?

THE WORKSPACE:

Where PII & PHI data (Electronic/Non-Electronic) is stored outside of the Network

Online Tax Payment

According to the FBI – Identity Theft is the fastest growing white collar crime in America.

THE NETWORK:

Where PII & PHI data is stored Electronically

What is Cyber Risk? Network Security & Privacy

The CONVERGENCE of TECHNOLOGY with INFORMATION

Information & Data is Valuable:

Advancements in technology have enabled organizations to capitalize on the value of Information & Data

Ease of Business:

Technology has made storing and removing data easy and convenient (Laptops, back-up drives, thumb drives, recordable CD's, iPads, Smartphones, the cloud, EVERYTHING…….)

The most vigilant Network Security and Privacy Policies are Vulnerable to Hackers, Rogue Employees, Independent Contractors, and Human Error!

HIGH FREQUENCY INDUSTRIES

2013	2012	2011	2010	2009	2008	2007
619 Published Breaches as of 12/31/13	447 Published Breaches as of 12/31/12	414 Publicized Breaches Reported Annually	662 Publicized Breaches Reported Annually	498 Publicized Breaches Reported Annually	656 Publicized Breaches Reported Annually	448 Publicized Breaches Reported Annually
57,868,922 Records Exposed	17,317,184 Records Exposed	22,945,773 Records Exposed	16,167,542 Records Exposed	222,477,043 Records Exposed	35,691,255 Records Exposed	127,000,000 Records Exposed
(40 Million Target)				(Heartland incident)		(94 Million from TJX incident)
2013 Breach by Industry	2012 Breaches by Industry:	2011 Breaches by Industry:	2010 Breaches by Industry:	2009 Breaches by Industry:	2008 Breaches by Industry:	2007 Breaches by Industry:
Financial Banking						
3.7% of Breaches 1.4% of Records	3.8% of Breaches 2.7% of Records	7.0% of Breaches 2.7% of Records	8.2% of Breaches 30% of Records	11.4% of Breaches 0% of Records	11.9% of Breaches 52.5% of Records	7% of Records 6.9% of Records
Educational						
9% of Breaches 5.6% of Records	13.6% of Breaches 13.3% of Records	14.3% of Breaches 3.6% of Records	9.8% of Breaches 9.9% of Records	15.7% of Breaches 0.4% of Records	20% of Breaches 2.3% of Records	24.9% of Breaches 1% of Records
Govt./Military						
10.2% of Breaches 3.3% of Records	11.2% of Breaches 44.4% of Records	11.4% of Breaches 43.7% of Records	15.7% of Breaches 7.5% of Records	18.1% of Breaches 35.7% of Records	16.8% of Breaches 8.3% of Records	24.7% of Breaches 6.4% of Records
Medical/Healthcare						
43.1% of Breaches 8.1% of Records	34.5% of Breaches 12.9% of Records	16.3% of Breaches 20.5% of Records	24.2% of Breaches 11.6% of Records	13.7% of Breaches 5.1% of Records	14.8% of Breaches 20.5% of Records	14.5% of Breaches 3.1% of Records
All Other Business						
33.9% of Breaches 81.7% of Records	36.9% of Breaches 26.7% of Records	46.9% of Breaches 33.7% of Records	42% of Breaches 41% of Records	41.2% of Breaches 58.9% of Records	36.6% of Breaches 16.5% of Records	28.9% of Breaches 82.6% of Records

Source: Identity Theft Resource Center

Types of Data Held by State/Municipal/Local/County Governments

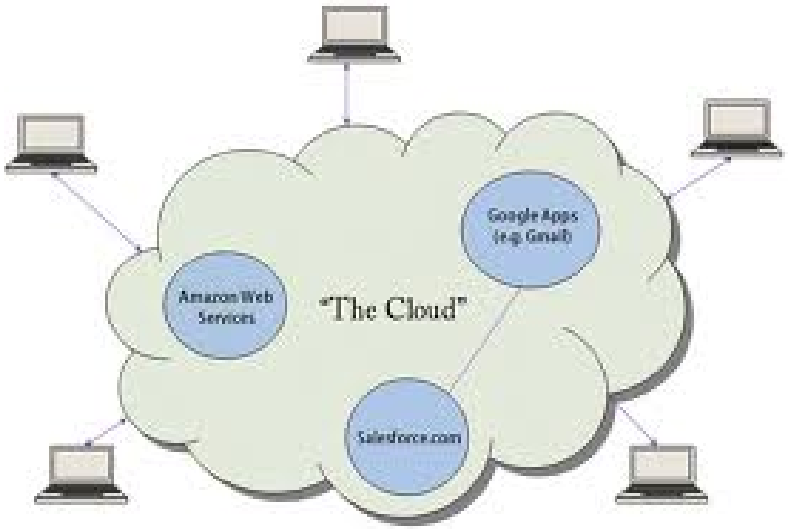
- State Agencies
- Census Data
- Corporate & Individual Tax Data
- Prison records
- Health records (e.g. VA, medical benefits programs)
- Contracting & Purchasing
- Immigration Records

- DMV Records
- State Employee Records
- K-12 & University Records
- Court Records
- FDOT
- Employee Records
- Police / EMT / Military Records

The REGULATORY LANDSCAPE is…complex, challenging and growing

- 50 State Privacy Laws (County/Local) - Laws or Regulation
- Foreign Privacy Laws – UK ICO – Information Commissioner's Office & many others (trans-border privacy issues)
  - *Federal Trade Commission*
  - *FACTA Regulation 114: Red Flags Rule*
  - *FERPA/DPPA*
  - *HIPAA / HITECH*
    - Standard for smooth, consistent, and secure electronic transmission of health care data.
  - *PII/PHI – personally identifiable information/health information about individuals - PII includes drivers license #'s, SS #'s, Credit Card #'s, address, account numbers & PIN's*
    - PHI includes written documents, electronic files, and verbal information. (Even information from an informal conversation can be considered PHI.)
      - *Examples of PHI include:*
        - Completed health care claims forms
        - Detailed claim forms
        - Explanations of benefits
        - Notes documenting discussions with plan participants
  - *SEC*
  - *PCI/DSS*

What About The Cloud?



Things to think about.

- Where is the data really stored?
- How is the data protected?
- What about the provider?
- Is the provider transferring data or moving your data around?
- Indemnification

HAS THE NEXT BIG LITIGATION TREND ARRIVED?

Social Media & Privacy - BYOD

What is your responsibility to safeguard, monitor and takedown information?

Litigation Trends

- Plaintiffs' Bar (Class Actions)
- Individuals (Identity Theft)
- Government (Privacy Laws)
- Impacted Businesses (Banks/Trading Partners)
- Third Parties

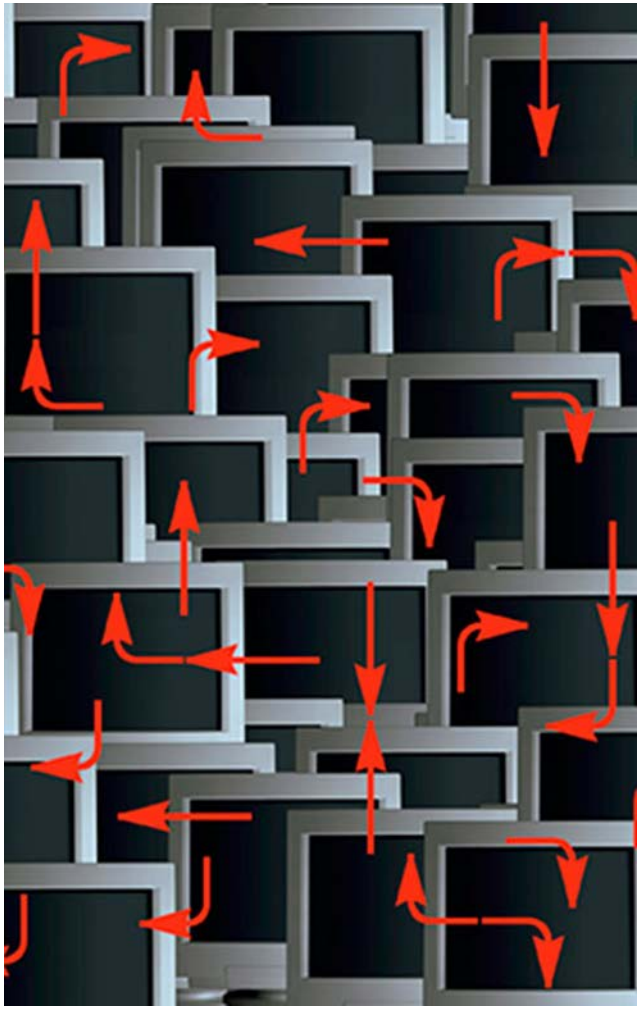
Immunities and Tort Caps

- Varies by state to state
- May or may not apply to Liability
- NO Applicability to notification requirements and other 1st party expenses
- Check with your appropriate legal representative on your states requirements
- F.S. 817.5681 exempts governmental agencies from administrative fines, but their contractors are still liable for fines of up to $500,000 for a failure to notify affected individuals

Loss Trends and Development

Privacy, Network and Data Breach Damages

- Costs of notification
  - *Forensic and legal investigation*
  - *Printing, postage, or other communication*
  - *Call Center*
  - *Credit Monitoring*
  - *Identity Restoration*
- Reputational damage
- Crisis management costs to restore reputation
  - *Legal, public relations, or other service fees*
  - *Advertising or related communications*
- Regulatory fines and penalties
- Legal liability
  - *Class action litigation*
  - *Financial institutions: card replacement*



Notification requirements often lie where the potential victim resides

Breach Examples

- **Department of Health FL 3/5/2014 - # 3,500**
- WFTV, the ABC affiliate in Orlando, reports that two health department employees took photos of such information as name, birthdate and Social Security number, and then sent the information to the brother of one of the employees who filed the fraudulent tax returns. They targeted patients ages 17 and 18 who were not likely to have filed returns. WFTV, citing indictments, reports that about 3,500 individuals were affected. Combined HHS.gov listing with HDM article in 3/2014.
  - *Rogue Employees*

- **University of South Florida – 9/9/2013 - # 140**
- Protected health information data breach by an employee. The person responsible for the data breach is no longer a university employee, said Anne Baier, spokeswoman for USF Health. How the personal information involving patients treated by USF physicians at Tampa General Hospital was obtained is under investigation. Baier said 140 patients were affected by the breach.. The breach was uncovered in late May 2013 when police pulled over the USF employee, identified only as a custodial worker, and searched the employee's car, finding patient information such as names, dates of birth and Social Security numbers. Patients possibly affected by the security breach were notified via a letter from USF in July.
  - *Theft of Data*

- **Department of Education FL - # 47,000**
- Personal information of roughly 47,000 teacher preparation program participants in the state was compromised for 14 days in late May, according to a statement Saturday by the Florida Department of Education.
  - *Data Breach*

Breach Examples

- **South Florida State Hospital FL Yes - # 1,000**
- Curtis Fullwood's job was to help patients with mental health problems find work they could do in the South Florida State Hospital in Pembroke Pines, but instead, authorities say, he stole their identities. Fullwood, 57, and his cousin, Terri Davis, 45, have pleaded not guilty to a federal indictment charging them with conspiracy to commit identity theft, conspiring to disclose individual's health information, access device fraud, wrongful disclosure of health information and aggravated identity theft.
  - *Theft of Data*

- **University of Florida - Shands Family Medicine - # 14,339**
- An employee working at a University of Florida medical clinic who had ties to an identity theft ring may have compromised patient personal and health information. UF is notifying 14,339 patients of the UF & Shands Family Medicine at Main practice that they should take appropriate measures to protect themselves from identity theft.
  - *Theft of data*

- **Department of Juvenile Justice - # 100,000**
- State law-enforcement officials are investigating a security breach at the Florida Department of Juvenile Justice that could affect the identities of more than 100,000 DJJ employees and youth offenders, state officials said Friday.
  - *Mobile Device not encrypted or protected*

What can you learn from past Privacy/Cyber events?

- Plan, Prepare, Practice
  - *Incident Response Team - (IRT/IRP)*
  - *Train Staff*
  - *Conduct event drills for the IRT/IRP*
- Know the rules
  - *Privacy regulations and guidelines*
  - *Identify applicable laws*
- Know your exposure
  - *Where does the data exist?*
  - *Superfluous data should not be collected*
  - *Internal/External third party reviews*
- Know your employees
  - *Education*
  - *Training*

What can you learn from past Privacy/Cyber events?

- Know your entity's network security risk
  - *Annual security risk assessments*
    - People/Processes/Technology
- Know your business partners
  - *Third parties/Independent Contractors*
  - *Inquire about policies and procedures*
  - *Indemnification*
  - *Responsibility to protect data*
  - *CONTAIN – the incident*
  - *RESPOND – based on findings from investigation*
  - *RESTORE – confidence in the organization*
  - *RETAIN – clients!*
- Manage Your Risk

CGL Policies……Now What?

COMMERCIAL GENERAL LIABILITY
FORMS FILING GL-2013-ODBFR

Access Or Disclosure Of Confidential Or Personal Information Exclusions Introduced

About This Filing

This filing introduces mandatory and optional exclusionary endorsements, for use with General Liability Coverage Part, addressing the access to or disclosure of confidential or personal information.

. GENERAL LIABILITY
CG 21 06 05 14

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

EXCLUSION – ACCESS OR DISCLOSURE OF CONFIDENTIAL OR PERSONAL INFORMATION AND DATA-RELATED LIABILITY – WITH LIMITED BODILY INJURY EXCEPTION

COMMERCIAL GENERAL LIABILITY
CG 21 07 05 14

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

EXCLUSION – ACCESS OR DISCLOSURE OF CONFIDENTIAL OR PERSONAL INFORMATION AND DATA-RELATED LIABILITY – LIMITED BODILY INJURY EXCEPTION NOT INCLUDED

Network and Privacy Insurance

Coverage & Gaps

	Property	General Liability	Crime / Bond	K&R	E&O	Cyber
1st Party Privacy / Network Risks						
Physical damage to Data only						
Virus / Hacker damage to Data only						
Denial of service attack						
B.I. Loss from security event						
Extortion or threat						
Employee sabotage of Data only						
3rd Party Privacy / Network Risks						
Theft / Disclosure of private info.						
Confidential corporate info. breach						
Technology E&O						
Media Liability (electronic content)						
Privacy breach expense / notification						
Damage to 3rd party's Data only						
Regulatory privacy defense / fines						
Virus / Malicious code transmission						

Coverage Provided?	
Coverage Possible?	
No Coverage?	

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

Available Coverage

Exposure Category		Description
Network Security Liability		Provides liability coverage if an Insured's Computer System fails to prevent a Security Breach or a Privacy Breach
Privacy Liability		Provides liability coverage if an Insured fails to protect electronic or non-electronic information in their care custody and control
Media Liability		Covers the Insured for Intellectual Property and Personal Injury perils the result from an error or omission in content (coverage for Patent and Trade Secrets are generally not provided)
Regulatory Liability		Coverage for lawsuits or investigations by Federal, State, or Foreign regulators relating to Privacy Laws
Crisis Management	Notification Expense	1st Party expenses to comply with Privacy Law notification requirements
	Credit Monitoring Expense	1st Party expenses to provide up to 12 months credit monitoring
	Forensic Investigations	1st Party expenses to investigate a system intrusion into an Insured Computer System
	Public Relations	1st Party expenses to hire a Public Relations firm
Data Recovery		1st party expenses to recover data damaged on an Insured Computer System as a result of a Failure of Security
Business Interruption		1st party expenses for lost income from an interruption to an Insured Computer System as a result of a Failure of Security
Cyber Extortion		Payments made to a party threatening to attack an Insured's Computer System in order to avert a cyber attack
Technology Services/Products & Professional Errors & Omission Liability		Technology Products & Services and Miscellaneous E&O can be added to a policy when applicable

3rd Party Coverage

- Network and Privacy Liability
  - *Coverage for:*
    - Claims arising from the unauthorized access to data containing identity information,
    - Failure to protect non-public information (PII/PHI/Corporate Confidential Information in your care, custody and control
    - Transmission of a computer virus, and
    - Liability associated with the failure to provide authorized users with access to the company's website

3rd Party Coverage

- Media Liability – Including online and offline Media
  - *Coverage for:*
    - *Claims arising online/offline content*
    - Libel
    - Slander
    - Defamation
    - Emotional Distress
    - Infringement of copyright/trademark/etc.
    - Invasion of Privacy

3rd Party Coverage

- Technology Products/Services Errors & Omissions
  - *Coverage for:*
    - Claims arising from the failure of a technology product or service to perform as indicated.

1st Party Coverage

- Crisis Management/Security Breach Remediation and Notification Expenses
  - *Coverage for:*
  - *Crisis Management Expenses*
    - Covers expenses to obtain legal assistance to navigate the event, determine which regulatory bodies need to be notified and which laws would apply
    - Public relations services to mitigate negative publicity as a result of cyber liability
    - Forensic costs incurred to determine the scope of a failure of Network Security and determine whose information was accessed
    - Notification to those individuals of the security breach
    - Credit monitoring
    - Call center to handle inquiries
    - Identity fraud expense reimbursement for those individuals affected by the breach

1st Party Coverage

- Computer Program and Electronic Data Restoration Expenses
  - *Coverage for:*
    - Expenses incurred to restore data lost from damage to computer systems due to computer virus or unauthorized access
- Cyber Extortion
  - *Coverage for:*
    - Money paid due to threats made regarding an intent to fraudulently transfer funds, destroy data, introduce a virus or attack on computer system, or disclose electronic data/information
- Business Interruption and Additional Expense
  - *Coverage for:*
    - Loss of income, and the extra expense incurred to restore operations, as result of a computer system disruption caused by a virus or other unauthorized computer attack

Cyber Insurance Market

A very robust insurance marketplace – expecting growth in 2014 – 40% (+/-)

Domestic and International

Value = Financial Loss Mitigation

- Expertise/Professionals
- Choice by Insured
- Breach Coach
- Preparedness Plans
- Security Audits
- eRisk Hub

Joe DePaul
Gallagher Cyber*Ris*k Services
101 John F. Kennedy Parkway
Suite 6
Short Hills, NJ 07078
973-939-3646
joe_depaul@ajg.com

thank you

Arthur J. Gallagher & Co.