Law firm Liability Exposures: How to protect your firm against Cyber Liability Claims

Mark Lefever, CIC, VP, Sales and Client Management
USI Affinity

Agenda

- Cyber Liability Exposures For Law Firms
- Cyber Risk Management Tips
- Cyber Liability Insurance

Cyber Exposures For Law Firms

Cyber Exposures – Law Firms Are Prime Targets

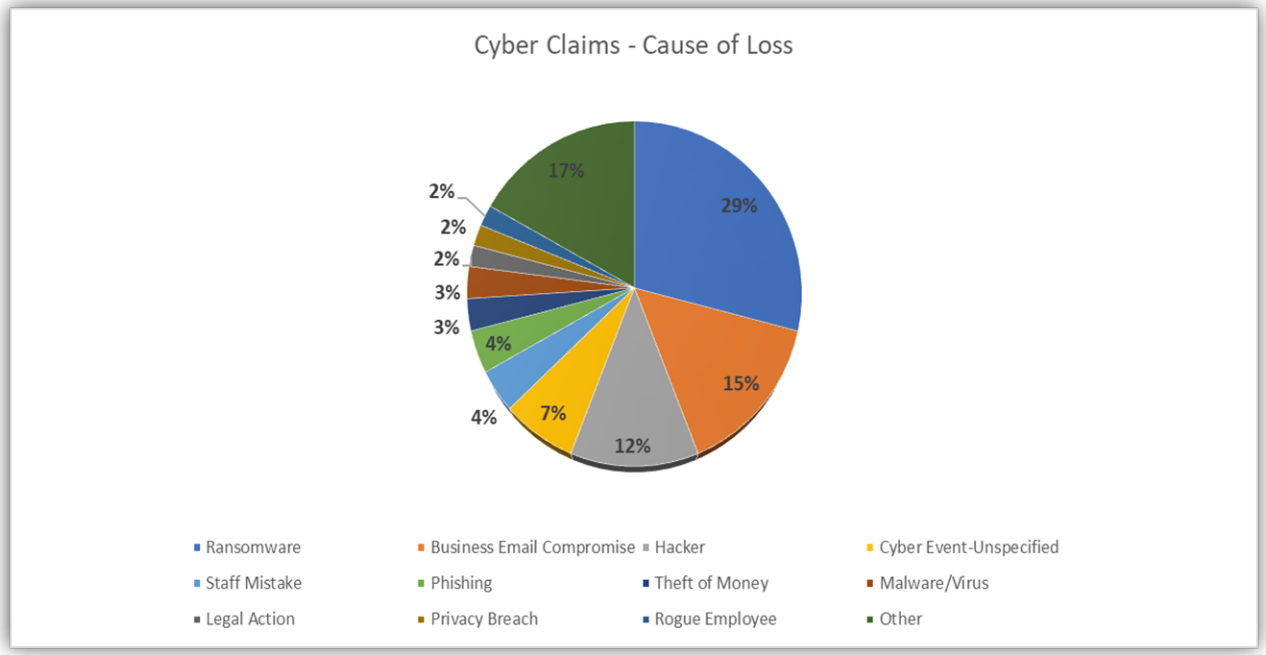
- Rich Collection of Data
- Sensitive Information
- Bank Information
- PII

- Poor Safeguards
- Lack of internal training and controls
- Lack of IT resources
- Wireless access
- Vendor Management
- Lost of stolen devices

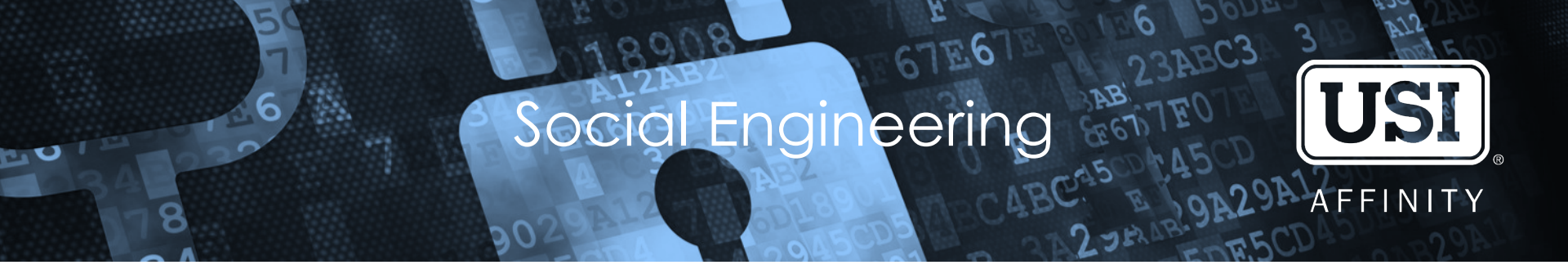
- Internal Exposures
  - Rogue employees
  - Careless staff

- External Exposures
  - Business associates, vendors and suppliers
  - Organized crime
  - Hackers

Cyber Claims



Source: 2022 NetDiligence Cyber Claims Study



Social Engineering

- Social Engineering is the psychological manipulation of legitimate users into performing actions, breaking security procedures, divulging confidential information and parting with tangible assets

- Social Engineering scams take advantage of the "human factor" to perpetrate a fraud

Social Engineering - NOT AN ISSUE FOR MY LAW FIRM

- **WRONG!**
- Roughly 26% of all law firms already victim of a data breach
- Roughly 51% of law firms have taken no measures to prevent data breach
- Roughly 50% have no data breach response plan
- Ransomware attacks occur every 10 seconds

Examples of Social Engineering Scams Involving Law Firms

- Misdirection of Escrow Funds
- Fraudulent court notices
- Fake job posting/resumes for review
- Bank account/LinkedIn/Netflix password reset/purported "unauthorized access"
- Email with incoming fax notification
- Misdirection of real estate closing costs
- Recent Examples of Ransomware Attacks:
  - 3 small SD Law Firms were subject to ransomware and threated to expose confidential data
  - TX boutique firm client data was released because of a ransomware attack

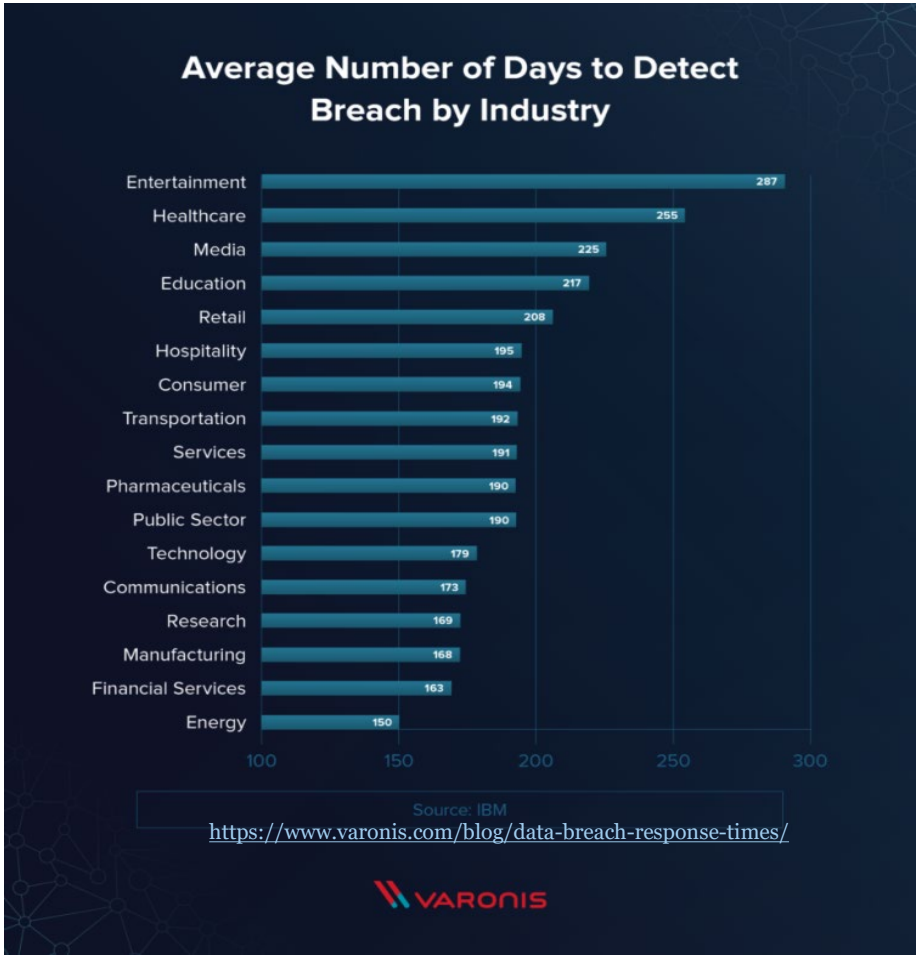
Why Are Small and Midsize Businesses Targeted?

- Small and midsize businesses (SMBs) are the principal target of cybercrime.
  - Based on one study, 60 percent of all targeted cyberattacks last year struck SMBs.
- SMBs are easier targets than larger organizations.
- Many SMBs lack sufficient resources and in-house expertise to address cyberattacks.
- It has been estimated that half of the small businesses that suffer a cyberattack go out of business within six months as a result.

Source: U.S. Securities and Exchange Commission, "The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses," 2015.

Breach Detection

- Obligation to Monitor For a Data Breach
- System Monitoring Activities



Stopping the Breach and Restoring Systems

Key findings:

Formation of the IR team lowered the total cost of a data breach by an average of $360,000 from the mean cost of $3.92 million.

$360,000

IR team lowers the total cost of a data breach by an average of $360,000

Extensive testing of the IR plan reduced the total cost of a data breach by an average of $320,000 from the mean cost of $3.92 million.

$320,000

IR plan reduces the total cost of a data breach by an average of $320,000

Organizations that both formed an IR team and extensively tested the IR plan saw the greatest savings – $1.23 million less than organizations that neither formed an IR team or tested the IR plan.

$1.23M

Savings from IR teams and testing the IR plan – $1.23 million less than organizations that neither formed an IR team or tested the IR plan.

Source - Ponemon Institute Cost of a Data Breach Study 2019

Cyber Exposure and the Need for Insurance

Cyber Exposures – Cyber Loss

- Loss or damage to data/information
- Loss of revenue due to a computer attack
- Extra expense to recover/respond to a computer attack
- Legal liability to others for computer security breaches
- Legal liability to others for privacy breaches (not just computers!)
- Regulatory actions and scrutiny
- Loss or damage to reputation
- Cyber-extortion
- Cyber-terrorism
- Management time expended on breach response

Your System has been breached, now what do you do?

USI AFFINITY

Breach Response Plan

Breach Counsel or Breach Coach

Insurance Carrier

Notify Your Clients and Provide Credit Monitoring

- Average cost is about $150 per client
- Every state has different rules and regulations
- Billable hours lost?

Forensics Team

- How you were breached
- Are they still in your system? If so remove them
- Recover any lost data
- Prevent breach from happening again

Cyber Extortion

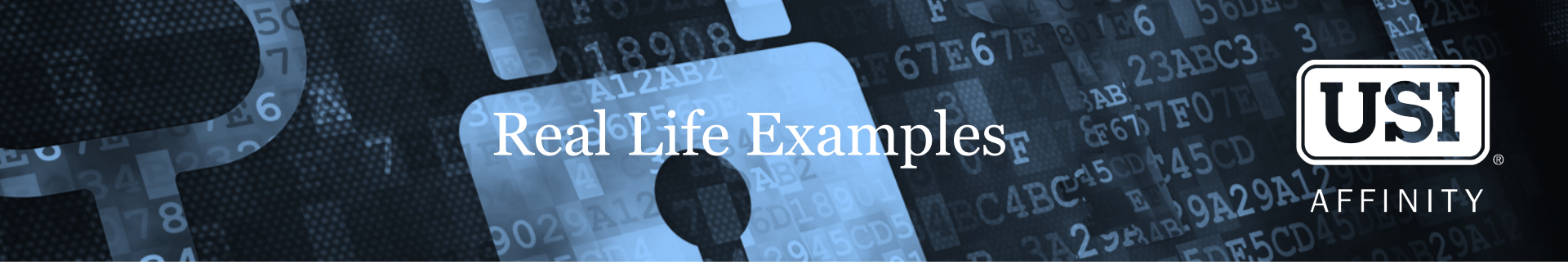
- Negotiate Rates, get your clients files back

Social Engineering/Fund Transfer Fraud

- Must have controls in place for this type of exposure

3rd Party Claims

- Notify Insurance Carrier, if not Cyber then Professional Liability



Real Life Examples

- The Fake Client
- The Fake Partner (Wire Transfer)
- The Blackmail Clients Files Held for Ransom and Total System Shutdown
- The new Firm Admin (Gift Cards for Clients)
- Debt Collections Agency
- Intercepting Voice Mails

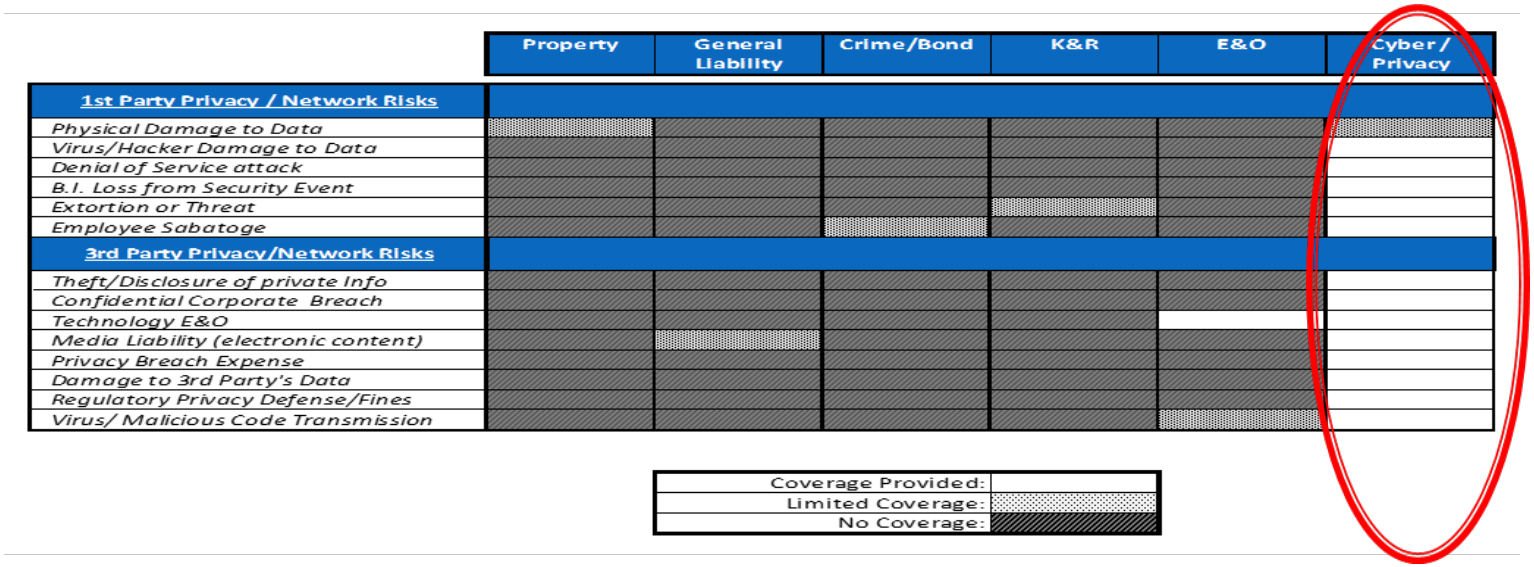
Cyber Exposures – How a Law Firm can Protect itself

- Buy Cyber Coverage!
- Incident Response Planning
- Employee Training
- Risk Analysis
- Encryption
- MFA
- Back-ups
- Document Retention Policy
- Penetration Testing
- Anti-virus and Patching
- Intrusion Prevention and Detection
- Vendor Risk Management

Risk Management

- Use common sense
- Avoid clicking on links in emails
- Utilize SPAM filters, malware detectors and anti-virus software
- Click on "details" for email address of sender
- Verify with a phone call to client/law firm
- Secure and frequent backups
- Changing password on frequent basis, complex passwords
- Continuous maintenance of operating systems and software programs
- Inform clients that wire instructions will not be sent over email, do not accept instructions over email

Insurance Coverage Gaps



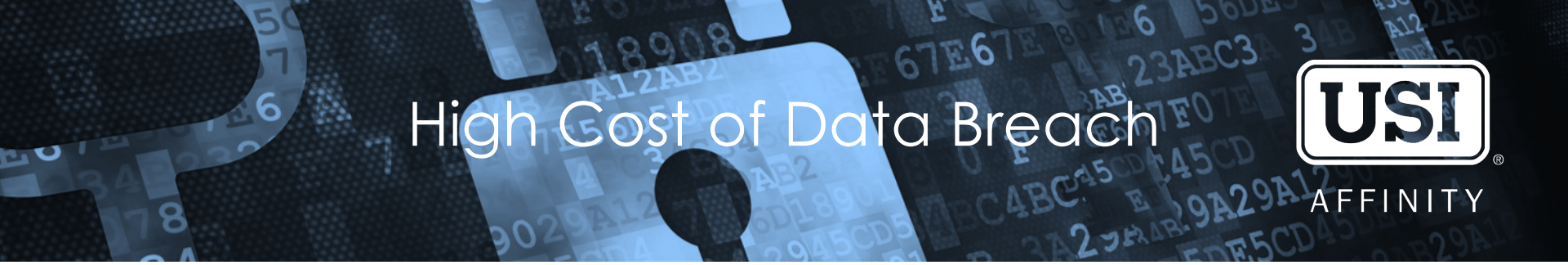
	Property	General Liability	Crime/Bond	K&R	E&O	Cyber / Privacy
1st Party Privacy / Network Risks						
Physical Damage to Data						
Virus/Hacker Damage to Data						
Denial of Service attack						
B.I. Loss from Security Event						
Extortion or Threat						
Employee Sabotage						
3rd Party Privacy/Network Risks						
Theft/Disclosure of private Info						
Confidential Corporate Breach						
Technology E&O						
Media Liability (electronic content)						
Privacy Breach Expense						
Damage to 3rd Party's Data						
Regulatory Privacy Defense/Fines						
Virus/ Malicious Code Transmission						

Coverage Provided:	
Limited Coverage:	
No Coverage:	

Traditional Insurance Gaps to name a few:

- Theft or disclosure of Third Party Information – GL
- Security & Privacy – "intentional act" exclusion – GL
- Data is not tangible Property – GL, Prop. and Crime
- Bi/PD Triggers – GL
- Value of Data if corrupted, destroyed or disclosed – Prop & GL
- Contingent Risks from external hosting, etc .

- Commercial Crime policies require "intent" and only cover "money securities and other Tangible Property"
- Territorial Restrictions
- Sublimits or long waiting periods applicable to any virus coverage available – Prop.



High Cost of Data Breach

IBM Security: Cost of a Data Breach Report 2022

$164 average cost for lost or stolen record for PII data

$4.35 Million→ Average cost of a data breach

$9.44 Million → Average cost of a data breach in the US

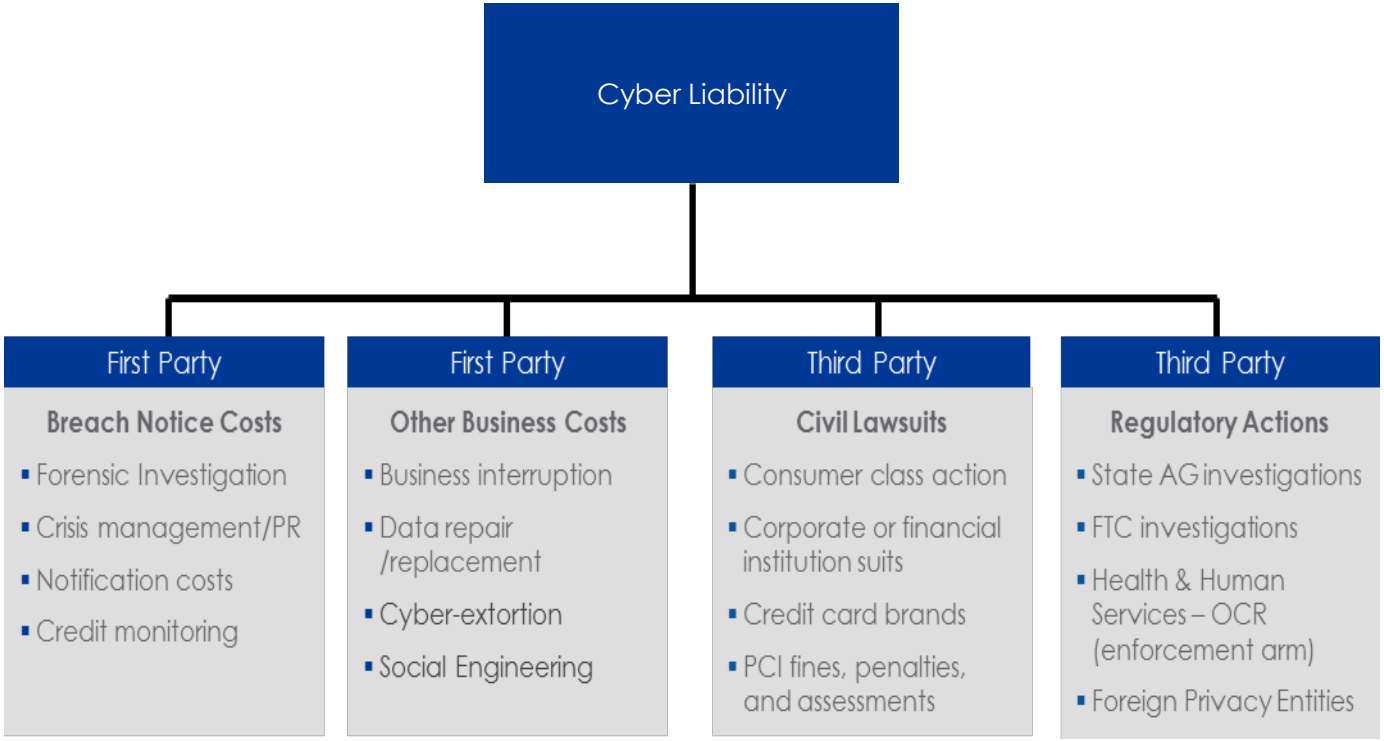
$1 Million → Average difference in cost where remote work was a factor in causing the breach

45% of breaches occurred in the cloud

83% of organizations studies have had more than one data breach

Compromised credentials responsible for 19% of breaches

What Does Cyber Insurance Cover?



Demand and Drivers for Cyber Insurance

- Demand for Cyber Insurance
  - Most insurance carriers have reported experiencing an increase in demand
  - Need for additional capacity
  - Policy terms and conditions are broadening
  - Additional sublimited coverage being offered
  - Co-insurance and Higher Deductibles

- Drivers for Cyber Insurance
  - Privacy Notification Laws
  - News of cyber-related events
  - Board/Sr. Management
  - Increased education
  - Experiencing a cyber-related loss
  - Contractual obligations

Insurance Application, Pricing and Coverage Details

Application Process

- Application focuses on security controls in place
  - MFA for Email, Remote Access, Network Cloud Administration
  - Maintain Weekly Backups
  - Funds Transfer Controls (secondary means of communication to validate)

Pricing

- Very Affordable for small firms
  - Deductibles from 1,000-5,000
  - Limits from 500,000-5,000,000

Coverages Listed on Quote

- Certain Coverages may be limited depending on your application
  - Cyber Extortion (co-insurance)
  - Funds Transfer Fraud (Sub-Limits)
  - Business Interruption (waiting period)

Questions

For any information on Professional Liability or Cyber Liability Insurance please feel free to contact:

Mark Lefever, CIC

mark.lefever@usi.com

717-572-2858

Vice President, Sales and Client Management

USI Affinity