Addressing Your Cyber Risk

Presented By:

Starke Agency, Inc. | Travelers Insurance

Jackson Thornton Technologies

In the News

Presented By:

Starke Agency, Inc.

Security in the News

1. **Target Corporation**
   - Massive breach involving POS systems
   - 40 million credit/debit card numbers stolen
2. **Home Depot**
   - Breach of POS Systems
   - Still too early to tell exact impact
3. **Community Health Systems**
   - 5.4 million patients information lost

We all know about the big corporation data breaches, but are you aware of the massive data breaches that occurred within small businesses?

Security in the News

1. **Sally Beauty Supply, Texas**
   - Type of Breach: Hack
   - People/Records Compromised: 282,000
   - Estimated Costs: $16,920,000
2. **El Agave Mexican Restaurant, Minnesota**
   - Type of Breach: Hack
   - People/Records Compromised: 200
   - Estimated Costs: $12,000
3. **Missouri Credit Union, Missouri**
   - Type of Breach: Unintended Disclosure
   - People/Records Compromised: 39,000
   - Estimated Costs: Unknown
4. **University of Delaware, Delaware**
   - Type of Breach: Hack
   - People/Records Compromised: 74,000
   - Estimated Costs: $4,440,000

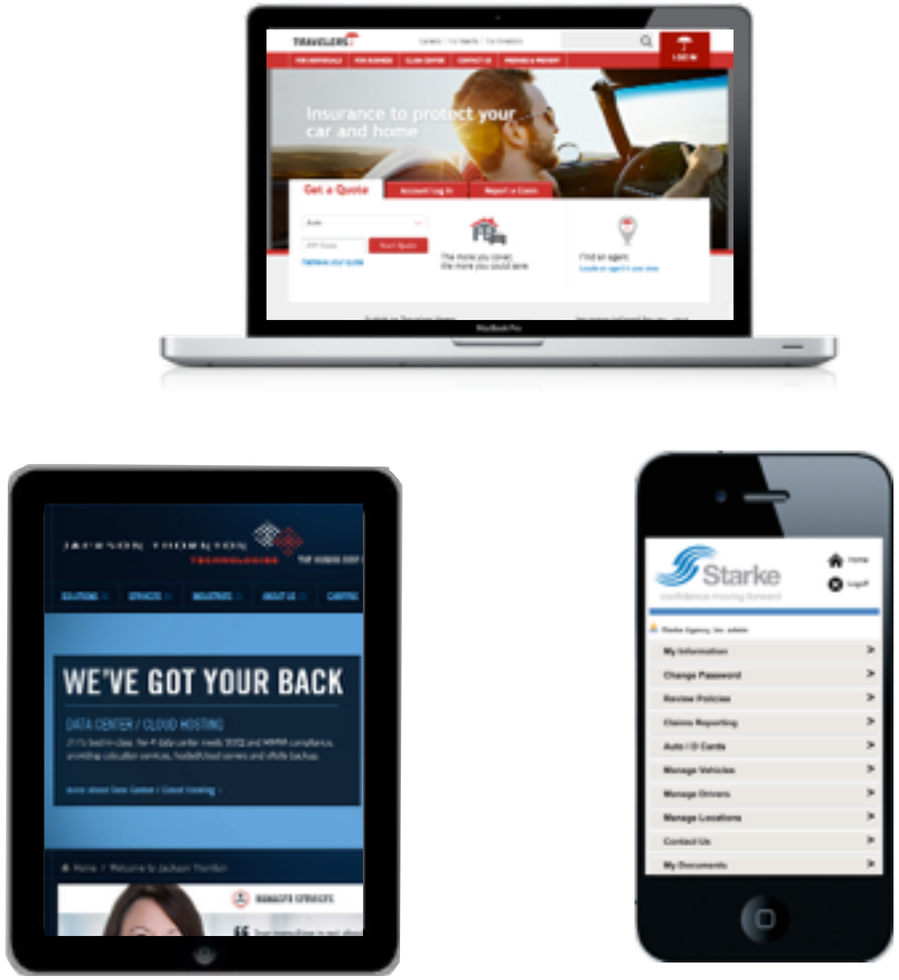
Protecting Your Data

Presented By:

Jackson Thornton Technologies

Data is Everywhere

1. Text files (word processors, Adobe, etc.)
2. Instant and text messages
3. Video (surveillance, cell phone, etc.)
4. Propriety applications and databases
    - Customer Service Systems
    - Billing Systems
    - GIS/Mapping Applications
    - Financial Management Applications
5. Audio (dictation, voicemail, etc.)
6. Portable/Remote Devices
    - E-mails
    - Cell phone/PDA data
    - Laptops and tablets


TRAVELERS
Insurance to protect your car and home
Get a Quote
WE'VE GOT YOUR BACK
DATA CENTER / CLOUD HOSTING
Starke

A Problem for Every Business

Got a computer? You’ve got Risk & Cost!

1. Since 2010, over 500 million data records have been compromised.
2. The number of U.S. data breaches tracked in 2014 hit a record high of 783.
3. Since 2007, there have been over 1 billion data records compromised
4. The average organizational data breach this year increased to $7.2 million, up seven percent from $6.8 million in 2014.
5. Several high-profile events in 2015 will increase this number.

Statistics

1. There are 556 million victims per year, 1.5 million victims per day and 18 victims per second.
2. Data breach statistics by industry:
   - Medical & Healthcare: 38.9%
   - Business: 35.1%
   - Educational: 10.7%
   - Banking & Financial: 5.3%
3. 43% of all U.S. companies experienced a data breach in the past year.
4. 71% of security breaches target small businesses (100 employees or less).
5. 68% of cyber attacks target retailers and restaurants.
6. 28,767 records are stolen on average per data breach.
7. $188 is the average cost per record stolen in a data breach.
8. Roughly 60% of small businesses will close permanently within 6 months of a cyber attack.

How is Data Compromised?

1. **External**

   - Viruses/Worms/Spyware
   - Key Loggers
   - Brute Force/Weak Passwords
   - USB Keys
   - Physical Removal
   - Mobile Devices

2. **Internal**

   - Intent → the most difficult to protect against

Types of Data Security Threats

1. **Network Security**
   - SQL Injection; Malware; Trojan Horses
2. **Physical Loss or Theft**
   - Lost or stolen laptop; Physical file security
3. **Cyber Extortion**
   - Gaining access to sensitive data and threatening to release
4. **Virus**
   - Can be a data breach, or just bring down network
5. **Denial of Service Attack**
   - Targeted attack to slow network

Identifying Your Cyber Risk

Presented By:

Starke Agency, Inc.

Risks

1. Financial
2. Reputational
3. Regulatory/Legal
    - 47 States have notice requirements/State Attorneys General
    - HIPAA and HITECH Acts/Other Federal Acts

Data Privacy Regulatory Environment

Federal Government Regulation:

- Three main cyber security regulations are:
    1. The 1996 Health Insurance Probability & Accountability Act (HIPPA)
    2. The 1999 Gramm-Leach-Bailey Act
    3. The 2002 Homeland Security Act, which included the Federal Information Security Act (FISMA)
- These three regulations mandate that healthcare organizations, financial institutions and federal agencies should protect their systems and information.

Data Privacy Regulatory Environment

State Government Regulation:

- In 2003, California passed the Notice of Security Breach Act which required that any company that maintains personal information of California citizens and has a security breach must disclose the details of the event. Personal information includes: name, social security number, driver's license number, credit card numbers and financial information.
- Several states have followed California's example and passed similar security breach notification regulations.
- 47 states have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.
- States with no security breach laws include: Alabama, New Mexico and South Dakota. However, expect to see an Alabama Notification Law proposed in the near future.
- If you have customers in another state, you will be expected to comply with that states notification laws.

Insuring Your Cyber Risk

Presented By:

Travelers Insurance

First Party Coverages

1. Security Breach Remediation & Notification Expenses:
    - Approved service provider
    - Reimbursement
    - Notice
    - Computer Forensics
    - Credit Monitoring
    - ID fraud expense reimbursement
2. Computer program and Electronic Data Restoration Expenses
3. Computer Fraud
4. Funds Transfer Fraud
5. Crisis Management Expenses
6. E-Commerce Extortion
7. Business Interruption

Third Party Coverages

1. **Network and Information Security Liability**

   *Providing coverages for:

   - Unauthorized access to identity information
   - Transmission of a computer virus
   - Blocked access for authorized users
   - Failure to provide notice of a security breach, where required by law

2. **Communications and Media Liability**

3. **Regulatory Defense Expenses**

Components of a Cyber Policy

Coping with the Breach/Restoration: Third Party Coverage

Insuring Agreement	Claim Scenario	Coverage Response
Network & Information Security Liability	A hacker successfully obtains sensitive, personal information from the insured's computer system. As a result, a number of customers bring a claim against the insured for allowing access to their personal information.	Damages and defense costs for covered lawsuits.
Communications & Media Liability	A lawsuit is brought against the insured by a competitor alleging that their online marketing content and product branding have been plagiarized and their trademarks infringed upon.	Damages and defense costs for covered lawsuits.
Regulatory Defense Expenses	An insured with offices nationwide suffers a major data breach involving thousands of customers. As a result, Attorneys General in multiple states bring a regulatory action against the insured.	Costs for responding to regulatory claims stemming from the data breach.

Components of a Cyber Policy

Coping with the Breach/Restoration: First Party Coverage

Insuring Agreement	Claim Scenario	Coverage Response
Security Breach Remediation & Notification Expense	A skilled cyber criminal hacks into the insured's internal processing system. Names, Addresses and credit card information for over 500,000 of the insured's customers are captured out of the system.	Costs for hiring a breach response firm to find and fix the breach, assist with notice requirements and expenses, provide credit monitoring and a call center for impacted individuals, and obtaining an ID Fraud policy for affected victims.
Computer Program & Electronic Data Restoration Expenses	A computer virus totally destroys the insured's operating system software and data.	Costs for repair and restoration of the insured's computer programs and electronic data.
Computer Fraud	An organized crime ring gains unauthorized access to the insured's accounts payable in their computer system, and alters the bank routing information on outgoing payments. The result: $1 million transferred to the crime ring's account.	Direct loss of the insured's money, securities, or other property.

Components of a Cyber Policy

Coping with the Breach/Restoration: First Party Coverage

Insuring Agreement	Claim Scenario	Coverage Response
Funds Transfer Fraud	The insured receives an email that appeared to be from its bank but was not. The insured's employee opened the email, which activated a computer virus called a Trojan Horse that read key strokes from their computer. The perpetrator used this means to obtain banking and password information and initiate a fraudulent electronic wire transfer from the insured's bank account.	The insured's funds that were fraudulently transferred from its bank account.
E-Commerce Extortion	The insured receives a series of notes which threaten to hack into its customer database and disclose all of the contact information to the general public.	Money or securities paid to the extortioner.
Business Interruption & Additional Expenses	A company's server is infected by a severe virus As a result, the insured's website is not available to customers for an extended period of time.	The net profit that would have been earned (or net losses that would have been avoided) resulting from the computer system disruption.

Risk Analysis
&
Disaster Recovery

Presented By:

Jackson Thornton Technologies

Elements of a Risk Analysis

1. Review existing security posture and compare against best practice and industry standard.

2. Identify and prioritize threats.

3. Assess impact on the loss of availability or integrity of your data

4. Create a remediation plan to take corrective action regarding any identified deficiency

Backup & Data Recovery Solutions

When evaluating solutions for backup & disaster recovery, here are some key things to consider:

1. Look for solutions with the shortest recovery times and facilitate the quickest recovery points at the lowest cost.

2. Understand the process by which systems are restored in the event of disaster. Know what is being backed up and what can be recovered.

3. Know your role in the backup process. Is it “set it and forget it” or does is require a manual intervention?

4. Consider text backup procedures. Can they be easily performed? Are they a true picture of the solution’ s ability to respond to disaster?

5. Vet any potential vendor thoroughly, and confirm regulatory compliance of any solution.

Bottom Line

Bottom Line

1. Consider third party contractual risk transfers:

- Insurance
- Indemnity & Hold Harmless Agreements
- Analysis of third party vendors.

2. Consider both administrative and technical methods of protection:

- Create policies and procedures that reflect your organizations commitment to protecting electronic data.
- Invest in technologies that enable enforcement of your policies.

3. The world of IT Security is ever-changing:

- Latest incidents show the size and scope of security threats continue to grow.

Bottom Line

4. Your electronically stored data is a liability:

- The goal is to minimize the risk of data loss and potential intrusion.

5. Plan for disaster:

- **Natural disasters:** Flood, tornado, fire, etc.
- **Hardware Disasters:** Disk Failure, Controller Failure, Board failure, Data Storage & Management Failure.
- Identify critical elements that must be recovered in the event of disaster.
- Determine your specific RTO and RPO.

6. Consider Independent Analysis:

- Assess your current position.
- Create a remediation plan and constantly work to improve security posture.