HF&C

HAYLOR, FREYER & COON INC.

Celebrating 92 Years

Cyber Liability – Proactive and Reactive Protection

Anto Almasian
Steve DeRegis

Insuring All You Value

HF&C
Haylor, Freyer & Coon Inc.

2020 Cyber Landscape

- Covid-19 Pandemic has accelerated cyber crime tremendously
  - Creation of an “Infodemic”
- 4,000 + maliciously registered domain names created containing “Covid” or “Corona” in the address
- Phishing emails are coming from “reliable” sources disguised as the CDC & WHO
- Every 14 seconds of the pandemic a business falls victim to ransomware
- 86% of breaches are financially motivated
- Threats seen in the first half of 2020 exceed all of 2019
- 60% of small businesses that experience a cyber attack go out of business within the next 6 months

Today's Top Targeted Industries

- Educational Services
- Healthcare
- Financial and Insurance Institutions
- Professional Services
  - Attorneys, Accountants, Architects, Engineers, Etc..
- Manufacturing

Today's Threats

- Human Error
- Malware
- Rogue Employee / Internal Actors
- Wire Transfer Fraud
- Phishing
- Vishing
- Cryptojacking
- Ransomware
- Social Engineering

HF&C
Haylor, Freyer & Coon Inc.

Human Error

- 22% of breaches are caused by human error
- Simple mistakes can have large consequences
- Examples:
  - Accidently publishing PII or PHI records
  - Leaving devices unattended
  - Emailing the wrong person / persons

HF&C
Haylor, Freyer & Coon Inc.

Ransomware Attacks

- Hijacking of a network or connected device(s) and held ransom for a payment usually demanded in cryptocurrency such as bitcoin
- 27% of all Malware incidents involve ransomware
- 18% of all organizations have blocked some sort of ransomware attack
- Has ripple effect consequences

HF&C
Haylor, Freyer & Coon Inc.

Vishing

- Increasingly used on Work From Home employees
- Usually used in conjunction with social engineering
- Adaptable style of attack
- Preys on vulnerable targets – elderly, new hires, performance based jobs, etc..

HF&C
Haylor, Freyer & Coon Inc.

Why Am I a Target?

- In a recent study of small to midsize businesses, 70% discovered an attempted attack on their network
- Unassuming businesses are easier targets
- Various methods of exploitation

HF&C
Haylor, Freyer & Coon Inc.

What's At Risk?

- **Financial Costs**
  - **$200,000** – Average cost of a breach to an uninsured small to midsize business
  - **$2,000,000 –** Average cost of breach to an uninsured a large business
- **Reputational Harm** – Do your clients trust you, will they again?
- **<$5,000** – Average cost of a Basic Cyber Insurance Program – $1,000,000 Limit

Common Sense Risk Management

Human Defenses – Create A Culture

- Basic Internet Safety Training
- Wire Transfer Procedures
- High Strength Passwords
- Employee Phishing Awareness

HF&C
Haylor, Freyer & Coon Inc.

Using Insurance Proactively

- Employee Training – Virtual Sessions
- Installing Firewall(s)
- Dual Factor Authentication
- Phishing Tests
- Dark Web Monitoring
- Cyber Security Vulnerability Assessments
- Privacy Regulatory Body Compliance Audits
- Virtual Private Networks (VPN's)

HF&C
Haylor, Freyer & Coon Inc.

What is Covered?

- Loss resulting from damage or corruption to insured's electronic data & computer programs
- Business Interruption – Loss of Income from the breach
- Customer or donor notification (state laws require notification)
- Credit monitoring (as required by law)
- Regulatory fines & penalties
- Public relations expenses
- Third Party Liability for causing a breach of someone else (Customer, Donor, Employee, Vendor, Bank, etc.)

What is Covered Continued

- No “Fire Department”
- Forensic IT Services (Crowd Strike, Cyber Scout)
- Extortion Negotiation & Resolution
  - Especially important for ransomware attacks

HF&C
Haylor, Freyer & Coon Inc.

Is All Cyber The Same ?

- Cyber Policies vs. Cyber Endorsements
- Cyber Policies differ carrier to carrier
- Polices can quickly become outdated

HF&C
Haylor, Freyer & Coon Inc.

Actual Claims

- Large School System – Ransomware attack – 58 servers encrypted – email and phone system disabled - $1.2 million paid in Bitcoin in 24 hours – 80% of data recovered
- Non-Profit had two separate fire walls – hackers penetrated the lessor fire wall – company decided to rebuild rather than pay ransom - $125,000 loss
- Trojan Horse (a virus used to capture a password) - Obtained CFO's password was able to conduct ACH transactions – 3 times with amounts totaling $1.4 million
- Large Municipality– employee accidentally published sensitive and private information to a webpage accessible by all district employees

Questions?

Anto Almasian, AAI
Haylor Freyer & Coon, Inc.
Risk Management Advisor
aalmasian@haylor.com
Phone: 315-703-1387
Cell: 315-250-0544
Fax: 315-703-7680

Steven G. DeRegis
Haylor Freyer & Coon, Inc
Senior Vice President
sderegis@haylor.com
Phone: 315-453-1726
Cell: 315-415-2001
Fax: 315-703-7683

Thank you for your time!

Sources Available Upon Request