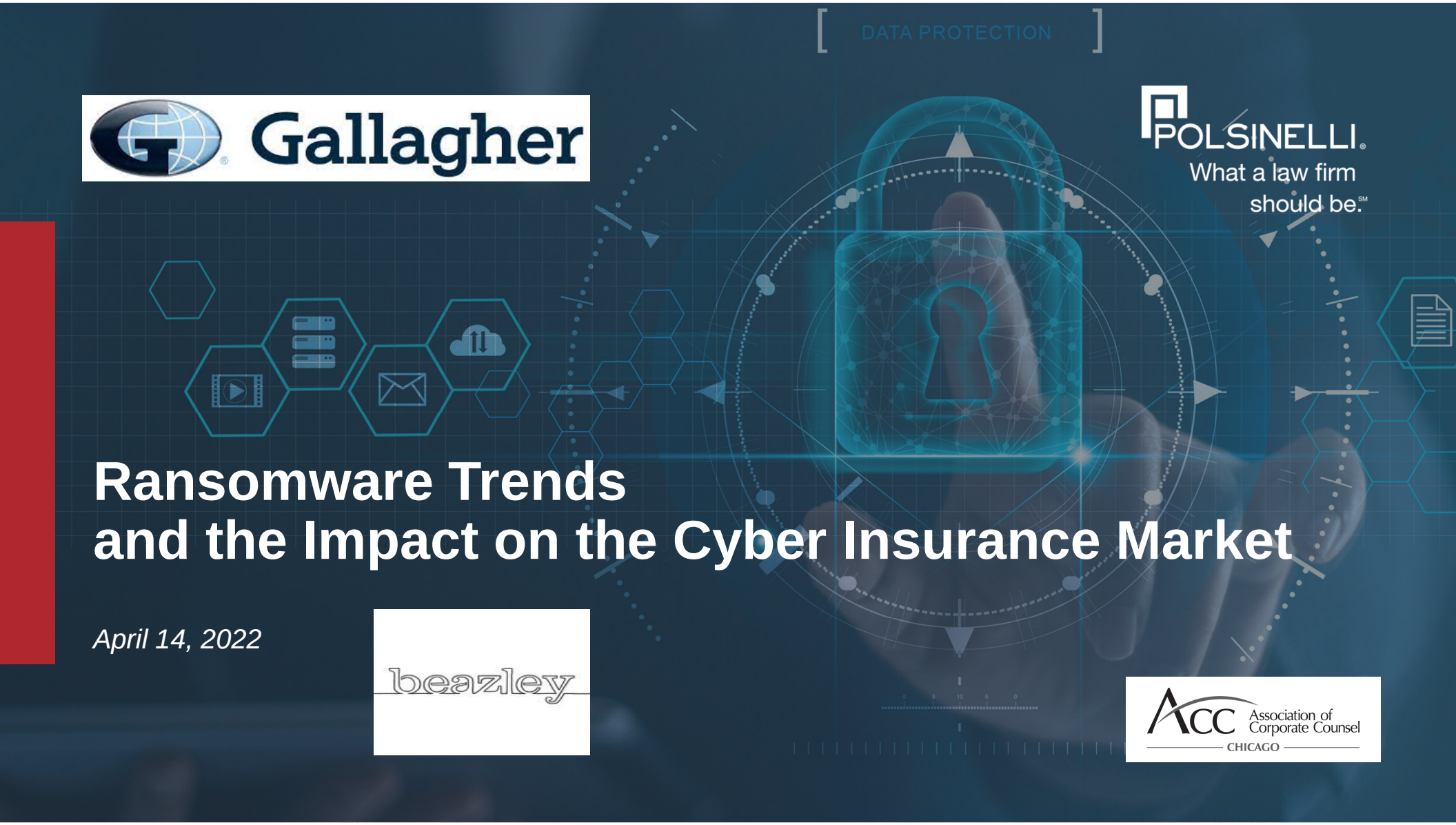

Gallagher

POLSINELLI
What a law firm should be.℠

Ransomware Trends and the Impact on the Cyber Insurance Market

April 14, 2022

beazley

ACC Association of Corporate Counsel CHICAGO

Sample Ransom Note

Attention!

| What happened?

We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You have a chance to get it back! It is easy to recover in a few steps.

We have also downloaded a lot of data from your network, so in case of not paying this data will be released.
If you dont believe we have any data you can contact us and ask a proof, also you can google [redacted]

When you pay us the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

| How to contact us and get my files back?

The only method to restore your files and be safe from data leakage is to purchase a unique for you private key which is securely stored on our servers.
To contact us and purchase the key you have to visit our website in a hidden TOR network.

Roles of Third Parties

- Insurance
- Legal Counsel
- Ransom Negotiator and Payment (OFAC)
- Data Forensic Firm
- Tech Vendor for Recovery
- Law Enforcement
- PR/Crisis Management
- Audit

Market Conditions: Cyber

2022 Cyber Insurance Marketplace

IT Supply Chain Attacks

- Solarwinds
- Acellion
- Microsoft Exchange
- Blackbaud

Ransomware

- Average Ransom Payment
- Exfiltration
- Phishing increases

Privacy Regulations

- GDPR
- CCPA / CPRA
- BIPA
- VDCPA
- Others in the works

Cyber Marketplace

Rate Increases

50 - 100% + for above avg controls
100 - 500% for below avg controls

Coverage Restrictions

Ransomware + Dependent Business Interruption –

- Coinsurance
- Sublimits
- Exclusions

Increased Retentions
Reduction of Capacity
Widespread Event Exclusions
Failure to Maintain Exclusion

Cybersecurity Controls Receiving Underwriter Attention

(Controls Potentially Preventing You From Securing Coverage)

- Require multi-factor authentication (MFA) for employee email
  - i.e., access to email on a non-owned/managed device
- Require MFA for remote access
  - Virtual Private Network (VPN), Remote Desktop Protocol (RDP)
- Require MFA for privileged accounts / privileged access
  - Domain admins, sys admin, etc…
- Require offsite (preferably offline) backups of critical data
  - Encrypted, cadence - less than 7 days for critical, 30 days minimum and tested at minimum once a year
- Create an audited written plan for patching critical software and hardware
  - Demonstrated capacity to apply critical security patches immediately, particularly in response to high profile zero day exploits (Microsoft Exchange, Kaseya, Accellion, etc.)

Cybersecurity Controls Receiving Underwriter Attention

(May Help You Secure More Competitive Pricing and Coverage)

- Employee Cybersecurity Training, including an phishing simulations that track performance
- Strong email filtering tools that block malicious attachments, suspicious file types, and executables. Additionally tools that can run suspicious attachments in a isolated environment or sandbox.
- Ability to articulate privileged access account security measures and/or an integrated PAM tool
  - Domain/service account restrictions across the environment and separate from day to day accounts
- EOL (End of Life/Unsupported) software and hardware segregated from the network and plans to decommission timely

Cybersecurity Controls Receiving Underwriter Attention

(May Help You Be Considered “Best in Class” Within Risk Profile Segment)

- Turn off local domain control on all owned/managed endpoints
- Password management (preferably through a vault or randomizer with limited access and check in/out)
- Provide detailed asset footprint of particular service accounts with domain credentials, the services they provide and how they are monitored throughout and between trees/forests
- Invest in a security information and event monitoring (SIEM) tool
- Invest in a tool that monitors data loss (DLP)
- Disaster Recovery/Incident response plan in place in the event of a cyber-incident that is tested and updated < yearly with key stakeholders
- Follow an information security framework (i.e., IS2700, NIST SP 800-53,171, CSF, CIS Controls, HITRUST and COBIT)