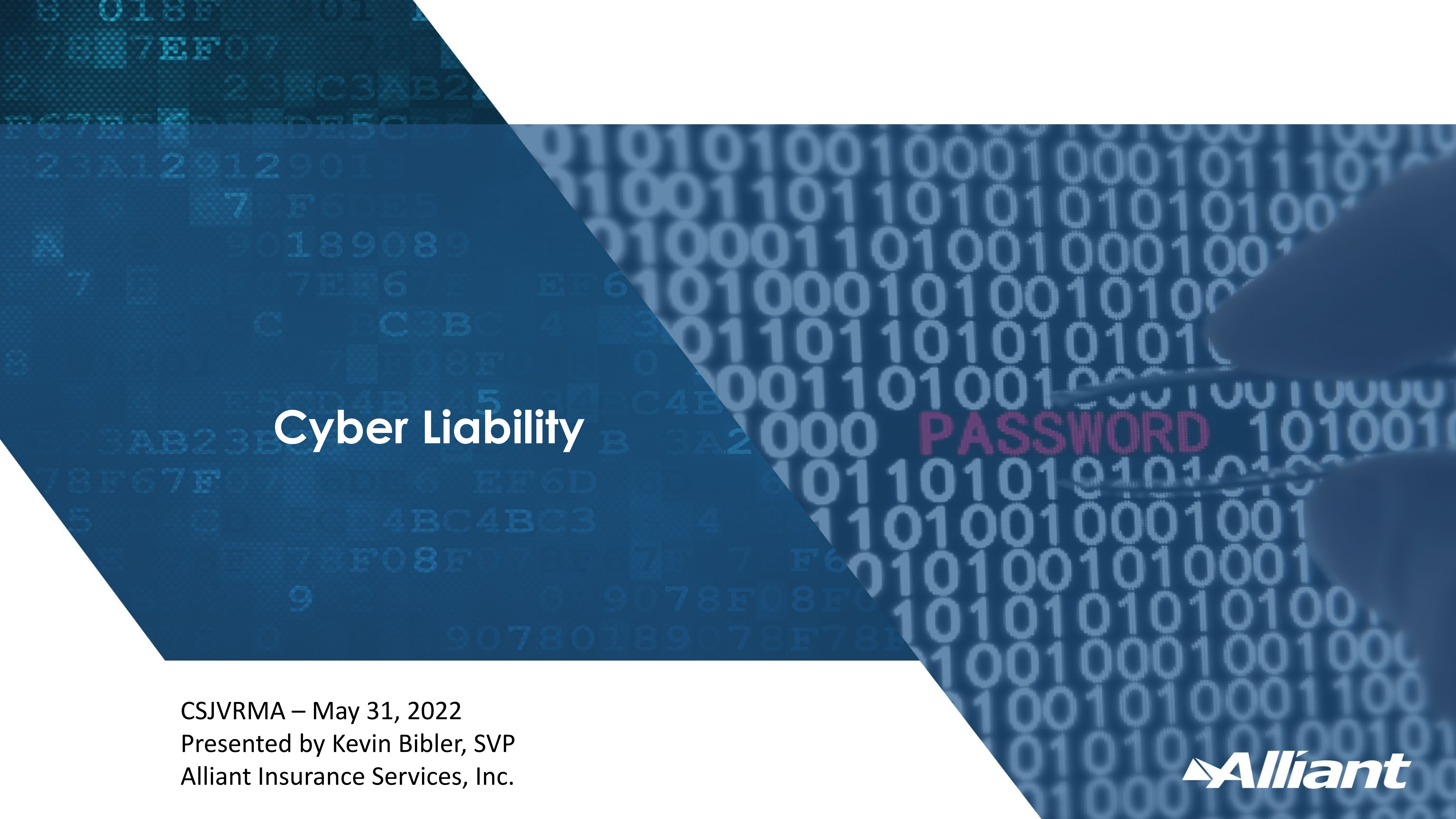
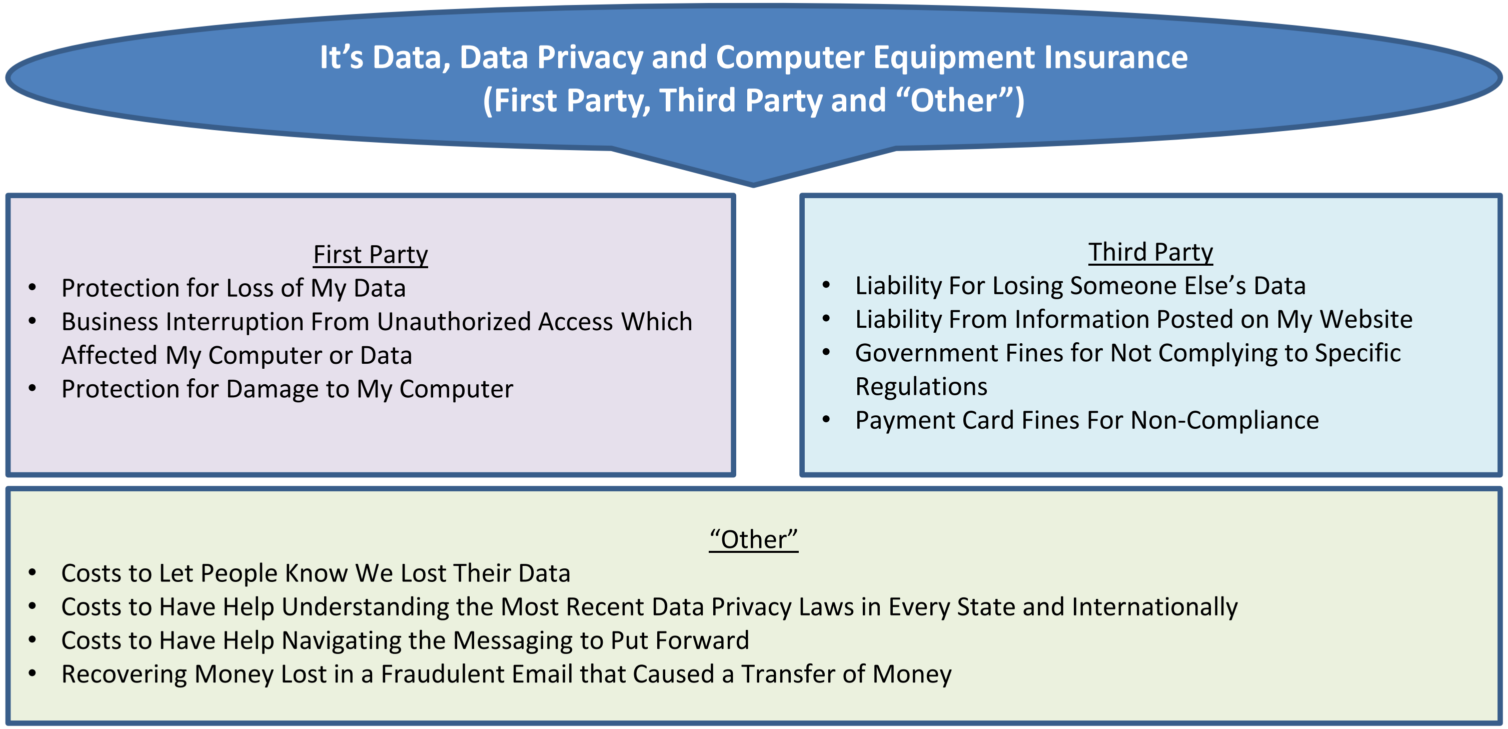
Cyber Liability



CSJVRMA – May 31, 2022
Presented by Kevin Bibler, SVP
Alliant Insurance Services, Inc.



It’s Data, Data Privacy and Computer Equipment Insurance (First Party, Third Party and “Other”)

First Party

- Protection for Loss of My Data
- Business Interruption From Unauthorized Access Which Affected My Computer or Data
- Protection for Damage to My Computer

Third Party

- Liability For Losing Someone Else’s Data
- Liability From Information Posted on My Website
- Government Fines for Not Complying to Specific Regulations
- Payment Card Fines For Non-Compliance

“Other”

- Costs to Let People Know We Lost Their Data
- Costs to Have Help Understanding the Most Recent Data Privacy Laws in Every State and Internationally
- Costs to Have Help Navigating the Messaging to Put Forward
- Recovering Money Lost in a Fraudulent Email that Caused a Transfer of Money

Breach Response

- Legal Services
- Forensics
- Notification
- Credit Monitoring
- Public Relations/Crisis Management

First-Party

- Business Interruption
- Cyber Extortion
- Data Restoration
- eCrime
- Bricking
- Cyrptojacking
- Reputation Loss
- Criminal Reward

Third-Party

- Data and Network Liability
- Regulatory
- Payment Card
- Media Liability

State of the Market

- Massive increase in the number of cyber incidents
  - $6 trillion impact going into 2021
  - Projected to hit $10.5 trillion annually by 2025
  - Was approximately $2 trillion in 2019

- The cyber security insurance market is expected to reach $20BN in 2025, registering a Compounded Annual Growth Rate of 20-25%, during the forecast period (2018 – 2025)

State of the Market:
Insurance Companies' Perspective/Feedback

- Top 10 cyber insurance carriers (controls about 70 - 75% of the marketplace) all report an overwhelming increase in ransomware claims
  - No industry class was spared
  - Public Entity was the most successfully targeted sector in terms of penetration by the attackers and frequency
    - Amongst the least prepared due to older software/computer equipment, lack of training, low IT security budgets

State of the Market:
Insurance Companies' Perspective/Feedback

- The Public Entity sector is now being viewed very closely by Insurance Company management, and continuing to tighten
    - Especially for large public entities and JPAs/Pools/Public Entities with Protected Health Information, carriers are worried about the vast number of members with the same ransomware exposure under the same policy
    - Many markets no longer writing new Public Entity cyber

What Does The Perspectives / Feedback Translate To?

Higher	Lower
Increase in Critical Examination of Risks	Lower Capacity
Retentions	Limits/Aggregate Limits
Premiums	Sublimits
Increased Request for Information	Less Expansion of Coverage Terms
Increase in Declinations	Less Accommodations

- How long will this last?
  - Only time will tell, next 12 months are critical to watch
  - If ransomware eases up and no other new form of loss takes its place, the industry could recover quickly…unlikely
- What should we be ready for?
  - Scans
  - **Minimum system requirements**

Minimum System Standards

- **Multi-factor authentication (MFA**) – 100% implemented for:
  - Remote access
  - Laptops
  - Privileged access
- **End-Point Detection (EDR)** –EDR protection, detection & response product implemented
- **Remote Desktop Protocol (RDP) –** Through Remote Desktop Gateway or secured VPN
- **Back Ups**
  - 1 working copy, 1 offsite, disconnected not working, 1 onsite disconnected not working
  - Tested at least twice a year
  - Ability to bring up within 24-72 hours – less time for critical operations (4 hours)
  - Protected with antivirus or monitored on a continuous basis
  - Encryption
- **Planning and Training**
  - Incident Response Plan
  - Business Continuity Plan
  - Social Engineering Training
  - Phishing Training
  - Training of account team staff on fraudulent transactions
  - General cyber security training
- **Patching –** Critical and High severity patches installed within 30 days, optimally within 7 days
- **Plan or adequate measures in place to protect end of life software**

Beazley Breach Solutions
Risk Management Portal

www.beazleybreachsolutions.com

WHAT'S ON THE SITE

Breach Response Services

Understanding the scope of services and expertise available to you.

How To Prepare

Steps your organization can take in order to minimize data breaches and their impact–including response plan template and sample policies—as well as resources for training employees.

Investigate

Overview of the varied components of an effective response – including a first responder guide and forensic tools.

Respond

Report an incident and look up breach notification laws specific to your state

For Beazley Breach Response inquires:

Steve Davidson (Steve.Davidson@Alliant.com)
Thomas Joyce (Thomas.Joyce@Alliant.com)
Susan Leung (Susan.leung@Alliant.com)

HOW TO ACCESS

FOR SINGLE MEMBERS

- Send email request to bbrservices@Beazley.com to obtain your organizations ***activation code*** – include the full names, email addresses and work addresses
- Beazley will send an email within 3-5 business days with your organization's activation code
- Go to beazleybreachsolutions.com and click ***"click here to register"***
- Enter your activation code, full name, email, industry, and create a password
- Click **submit**
- You will receive an email within minutes with a link to ***validate your registration***
- Click to validate, log in, and you're ready to go!

FOR JPA/POOL MEMBERS

- Provide a list of pool members (member name, risk management contact name and email), along with the full address of the JPA, to your Alliant Service Team
- Alliant will convert the information into the *Beazley template* and send the request to bbrservices@Beazley.com
- Within 3-5 business days, Beazley will send each risk management contact a welcome email with their organization's activation code
- Contacts should go to beazleybreachsolutions.com , click ***"click here to register,"*** and enter the activation code, full name, email, industry, and create a password *(remember; this will need to done for each domain name of the JPA/Pool)*
- Click **submit**
- The contact will receive an email within minutes with a link to ***validate registration***
- Click to validate, log in, and they're ready to go!

Cyber Questions?