PARKER SMITH & FEEK

An IMA Company

- COMMERCIAL INSURANCE
- EMPLOYEE BENEFITS
- PERSONAL INSURANCE
- RISK MANAGEMENT
- SURETY

CYBER

Markets in Focus

Insurance Pricing & Market Update

Q2 2022

Markets in Focus

TABLE OF CONTENTS

Markets in Focus

CYBER

Introduction

The Cyber insurance marketplace continues to be "hard" as Cyber carriers are consistently looking to right-size their portfolios due to 2020 and 2021 claims results. There is an ongoing emphasis on rate increases and "must have" technical security controls. The frequency of ransomware claims has slowed, but the severity factor remains amongst other exposures. While the underlying risk poses a volatile class, we continue to see the coverage evolve and this coverage is now deemed critical and essential to every organization's overall risk management strategy.

Claims

The volume of successful ransomware claims has decreased.[1] That decrease can be attributed to multiple factors:

+ Increase in global law enforcement cooperation
+ High profile events provided a wakeup call for many organizations that had never viewed themselves previously as a target, and thus forced them to improve security hygiene
+ The cyber insurance renewal process is structurally mandating better security and continuity to maintain coverage

Due to successful implementation of mitigating controls (e.g., backups), many targeted organizations have been able to avoid paying ransom demands. This has prompted a change in adversarial tactics, with extortionists resorting to publicizing confidential organization information. This can dramatically alter the nature of an attack, resulting in a data breach and associated expenses.

While the volume of attacks has decreased, the size of ransoms has increased.

+ Average Ransom Payment $322,168 (+130% from Q3 2021)[1]
+ Median Ransom Payment $117,116 (+63% from Q3 2021)[1]

84% of Ransomware attacks in Q4 2021 included data exfiltration[1]

Much of the focus and emphasis has been on payments. However, cyber carriers continue to point to Business Interruption as their greatest area of concern when considering Ransomware.

The average case duration of Business Interruption in Q4 2021 was 20 Days (-9% from Q3 2021)[1]

While outsourcing can increase efficiencies, we continue to see an increase in claims emanating from supply chain attacks (e.g., your vendor has been hacked).

+ Software supply chain attacks grew by more than 300% in 2021 compared to 2020, according to a study by Argon Security

The decrease in ransomware attacks has coincided in a substantial uptick on social engineering attacks. Fraudsters can steal funds by duping employees or customers.

Underwriting & Rates

We are seeing rate increases on average between 30 – 40%*. Rate is being driven by three factors:

1. Industry
2. Technical security controls
3. Prior loss activity

Carriers continue to require a supplemental application specific to security controls surrounding the mitigation of ransomware. Specific areas of focus include:

+ Multi Factor Authentication (MFA)
  - » Remote access
  - » Privileged users

+ Enterprise implementation of Endpoint Detection & Response (EDR) solution

+ Data backup procedures: Questions asked include:
  - » Disconnected from the network or cloud based?
  - » Encrypted?
  - » Restricted access?
  - » Tested?
  - » Multiple copies?

+ Software patch management to ensure critical security patches are made within 30 days

+ For our RENEWAL PREP CHECKLIST, go to: imacorp.com/cyber-checklist

In addition, carriers are inquiring about ongoing potentially large-scale vulnerabilities such as Log4j.

Insureds not having satisfactory controls in place may see non-renewals, substantially higher rate increases or a reduction in coverage. This reduction may come in the form of sub-limits or co-insurance provisions.

Cyber carriers are looking to reduce exposure to business interruption by reducing limits and increasing waiting periods to trigger coverage.

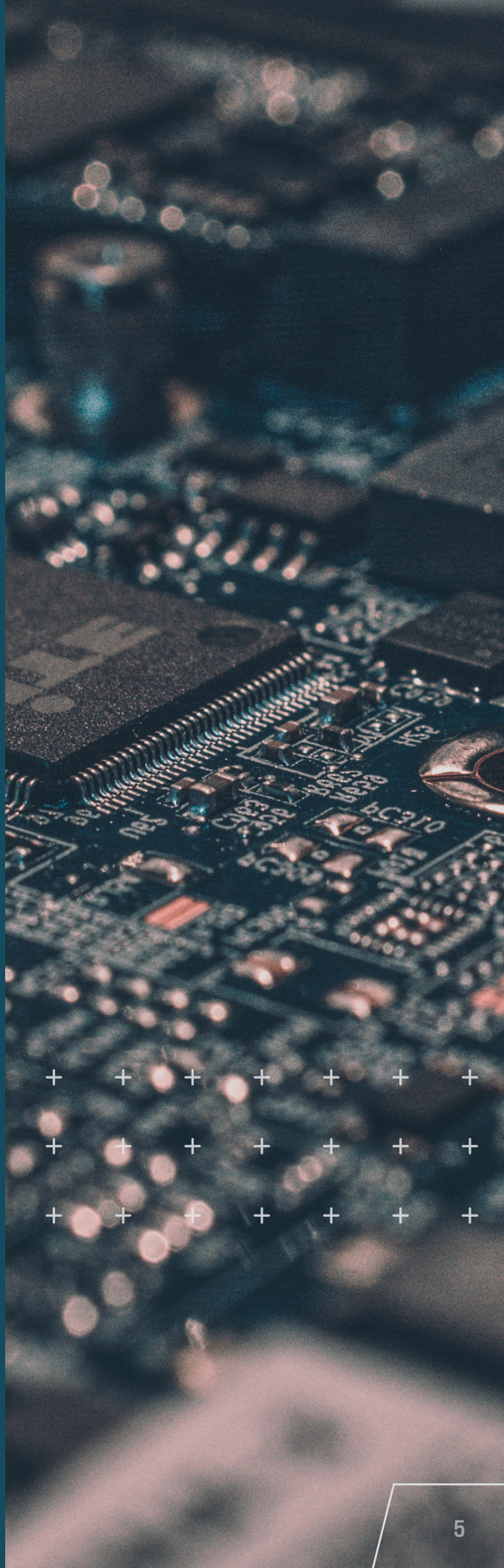
Market Trends

+ With limited exceptions, we are seeing insurance companies remaining committed to the cyber marketplace

+ We continue to see new "insurtech" market entrants. These new providers can provide more technical solutions and add competitive options for consideration

+ While there are legitimate concerns related to the Russia/Ukraine conflict, there has yet to be substantial carryover into cyber insurance claims activity

+ Continued emphasis on minimizing "Silent Cyber" exposures. "Silent Cyber" is an issue where cyber perils are unintentionally triggering standard Property & Casualty policies



[1] *Coveware Ransomware Quarterly Report (2.28.22)*

MORE THAN JUST INSURANCE

Parker, Smith & Feek is a diversified financial services company specializing in risk management, insurance, employee benefits and wealth management. It is the third-largest privately-held and employee-owned insurance broker in the country and employs more than 1,700 associates.

PARKER SMITH & FEEK
An IMA Company

EDITOR-IN-CHIEF

JOHN SEEGER, Director of Marketing, Market Intelligence & Insight

MARKETS IN FOCUS CONTRIBUTORS

TIM BURKE, Director of Cyber Risk

AUTUMN STONE, Cyber Specialist

www.psfinc.com