INSUREtrust

BCFGroup™
Insurance Redefined™

Cyber Insurance

What you need to know….

April 2021

BCF Group™
Insurance Redefined™

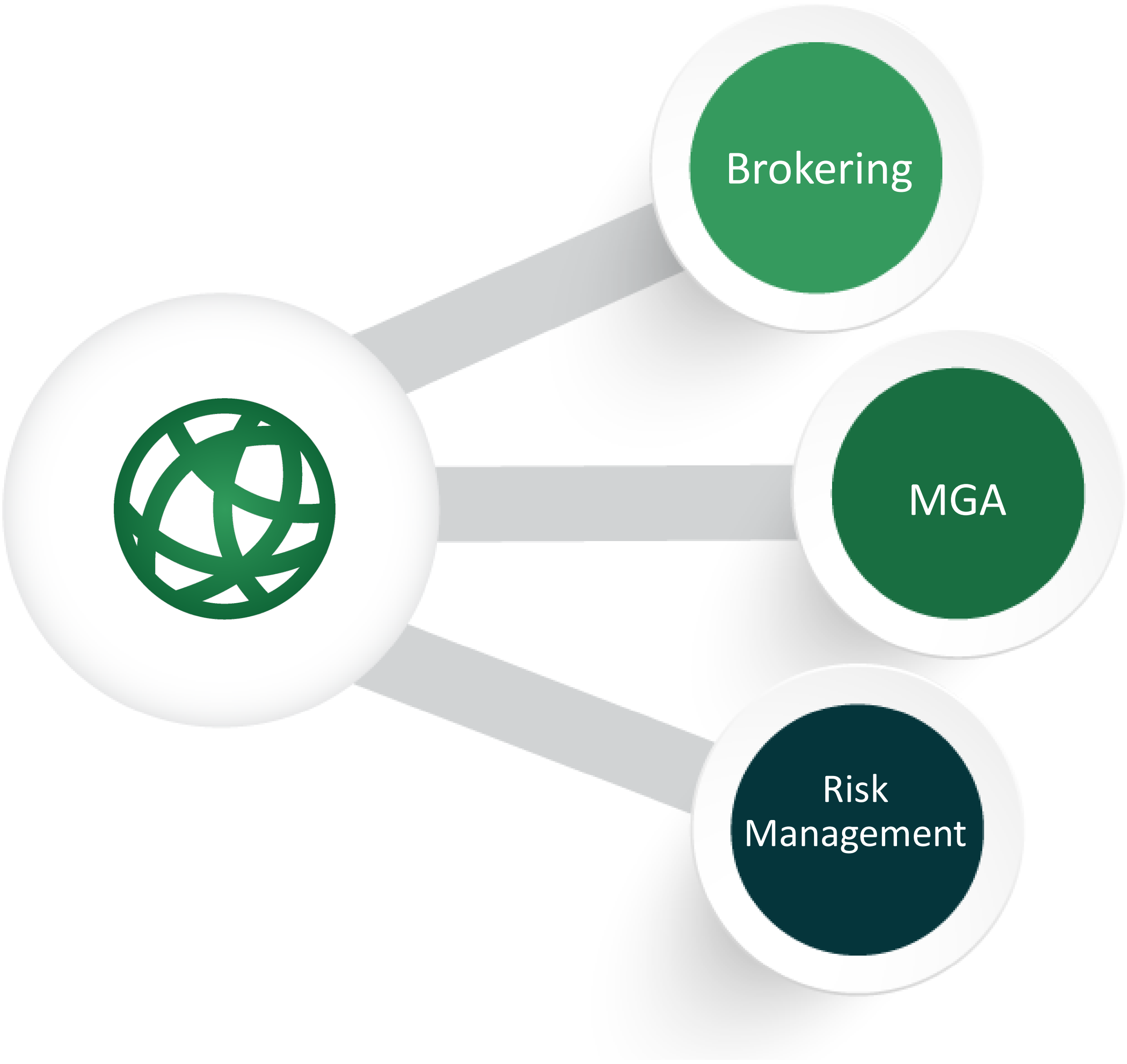
Departments

- ➢ Business Insurance
- ➢ Personal Insurance
- ➢ Employee Benefits

Our Purpose

- ➢ We care for people
- ➢ We serve people
- ➢ We solve, or prevent problems for
- ➢ people
- ➢ We make life easy for people

Trent Hess, CIC, CRM, ACRA
Business Insurance Professional



Who is INSUREtrust?

Cyber Industry Pioneers – 1997

Advisen Cyber Broker of the Year – 2017, 2019 & 2020 (wholesale)

Advisen Cyber Person of the Year (USA) – 2018

Making Cyber Simple. Really.

Agenda

What Does Cyber Insurance Cover?

Cyber Claim Loss Trends

Best Practices Pre-Incident

Prepare & Mitigate

Best Practices Post-Incident

Adopt & Protect

Emerging Cyber Threats

Overview/ Q&A

What Does Cyber Insurance Cover?

1. Incident Response / 1st Party Costs
2. Cyber Crime
3. Cyber Extortion (Ransomware)
4. Business Interruption & Extra Expense
5. Network & Internet Security Liability
6. Privacy Liability
7. Regulatory Coverage
8. Content/Advertising Liability

Cyber Claim Loss Trends

- In Ryuk ransomware attacks, the average ransomware payment was over $1M.
- Phishing remains one the most common access points for hackers.
- Average payment has more than doubled in the first 6 months of 2020, peaked at $239K in Q3. Q4 saw a decrease to $154,108.
- The most attacked sector of companies as of Q4 2020 are those with 11-100 employees (about 30% of the attacks) and the median size is 234 employees which was up 39% from Q3.
  - **75% of attacks are on companies of $50M in revenues and under**.
- Data Exfiltration happens more often than not in attacks.
  - 70% of Ransomware attacks in Q4 Involved the threat to leak exfiltrated data
  - Fewer companies are giving in and paying the extortion demand.
    - In Q3, 74.8% of companies that were threatened with a data leak opted to pay. In Q4, that percentage declined to 59.6%.

Cyber Claim Loss Trends

- The 4th quarter of 2020 marked a turning point with the data exfiltration tactic.
  - Coveware continues to witness signs that stolen data is not deleted or purged after payment.
  - Groups taking measures to fabricate data exfiltration in cases where it did not occur

- A concerning trend is the increase in the incidence of irreversible data destruction as opposed to just targeted destruction of backups or encryption of critical systems.

- In Q4 2020, multiple reports that entire clusters of servers and data shares had been permanently wiped out, with no recourse for retrieving the data even with the purchase of the decryption key.

- The uptick in haphazard data destruction has led some victims to suffer significant data loss and extended business interruption as they struggle to rebuild systems from scratch.

Source:www.coveware.com

Best Practices Pre-Incident

- Implement minimum security standards
  - Two factor authentication
  - Segregation of backups from the network
  - Limit sensitive data privilege and requiring authentication
  - Have an incident response plan and test it
  - Secure network access points
- Vendor risk management
- Familiarizing yourself with your legal counsel that comes with your Cyber policy
- Keeping employee awareness and training standards high
- Knowing where your most sensitive data is and limiting aggregation

Best Practices Post-Incident

Adopt Learnings & Protect Enterprise

- Use forensic findings as a blue-print for immediate return on investment
- Update your Incident Response Plan
- Do a table-top of your past incident, update plans again
- Consider better cloud-based solutions (if applicable)
- Hire a project manager to implement post-incident findings

Other Evaluations

- Did you have the right level of insurance?
- Claims Experience | Vendor Experience | Retainers

Emerging Cyber Insurance Trends

- Increased Underwriting
- Use of scanning technology
- Supplemental Ransomware Applications
- Limiting capacity
- Increased retentions
- Sub-limits and co-insurance

First Party Cyber Coverages

Incident Response	Cyber Extortion	Business Interruption/ System Failure	Cyber Crime
• Privacy Counsel/ Breach Coach	• Ransomware	• Loss of Income while non-operational	• Social Engineering/ Phishing
• Forensics	• Ddos Attacks	• Extra Expenses	• Invoice Manipulation
• Notification	• Data Exfiltration	• Contingent BI/SF	• Utility Fraud/ Cryptojacking
• Credit/Identity Monitoring		• IT only or All Critical	• Telecom Fraud
• Public Relations		• Bricking-property damage	• Funds Transfer Fraud

Third Party Cyber Coverages

Network Security	Privacy	Regulatory	Media
• Failure of Network Security	• Unauthorized access or loss of private information	• Privacy/Identity Laws	• Infringement of intellectual property
• Transmission of Virus or Malicious Code	• PII, PHI, CCI	• Local	• Advertising & Personal Injury
• Ddos attacks		• State	
		• Federal	
		• International	
		• Defense, fines & penalties	

Questions?

INSUREtrust

BCFGroup™
Insurance Redefined™

Erin Burns| *EVP, Head of Brokerage Operations*
INSUREtrust
O: 770-200-8000 x131
M: 804-301-3978
eburns@insuretrust.com
www.insuretrust.com

Trent Hess, CIC, CRM
Business Insurance Professional, BCF Group

t: 717-560-7730 | 800-732-3556 |m: 717-575-9033
f:717-560-8369
e: trenth@bcfgroup.net | w: www.bcfgroup.net
a: 2101 Oregon Pike, Ste. 300, Lancaster, 17601