GEAPS EXCHANGE

KANSAS CITY • 2022

Stay Connected!

Download the "*GEAPS Exchange*" app for schedule, maps and surveys.

Share on Social!

#GEAPSExchange

Wifi Network: GEAPS2022 Password: Exchange92

Thank you to our Education Program Sponsors!

Cargill®

CCSGroup
Custom Concrete Specialists

GEAPS
Great Plains Chapter

Grain Journal

MKC
Shared growth.
Shared success.

Sii Specialty Industries Inc.

Cyber Security for the Grain Industry

GEAPS EXCHANGE
KANSAS CITY • 2022

Dan Hanson,
CPCU, MBA, CCIC

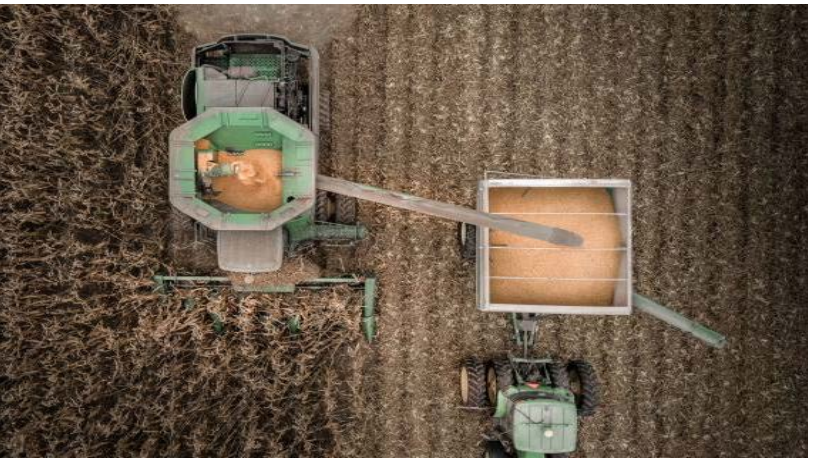
Marsh McLennan Agency

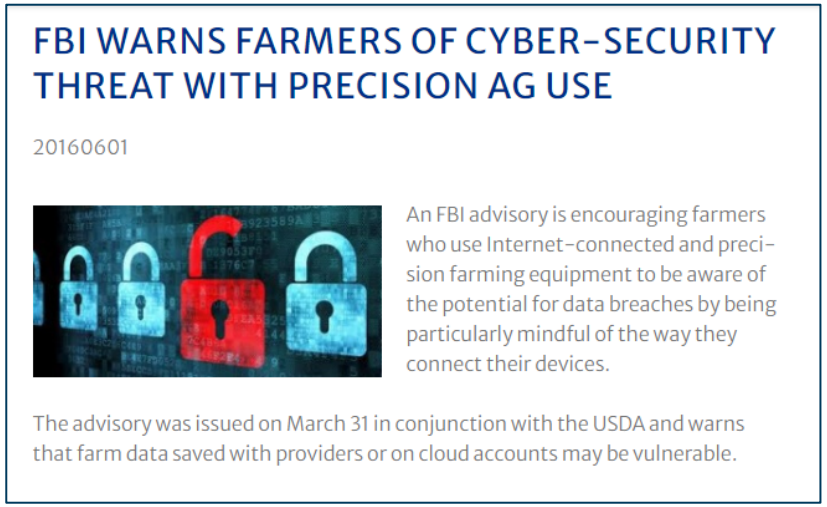
Senior Vice President, Management Liability & Client Experience

MarshMcLennan Agency

Cyber Security for the Grain Industry

GEAPS EXCHANGE
KANSAS CITY • 2022





US Farm Co-ops Urged To Improve Security After Cyber-attacks

Iowa's New Cooperative and Minnesota's Crystal Valley both suffered Russian ransomware attacks, prompting concern over national supply chain infrastructure

Vilsack urged U.S. agricultural cooperatives to "harden" defenses against cyber attacks.

Bloomberg,
Sept. 22, 2021

Cybersecurity Report: "Smart Farms" are Hackable Farms

Net- and IoT-connected agriculture could help feed 8.5 billion by 2030 – but also may be broadly vulnerable to cybersecurity threats

Why Agriculture?

What is a Good Target for a Cyber Criminal?

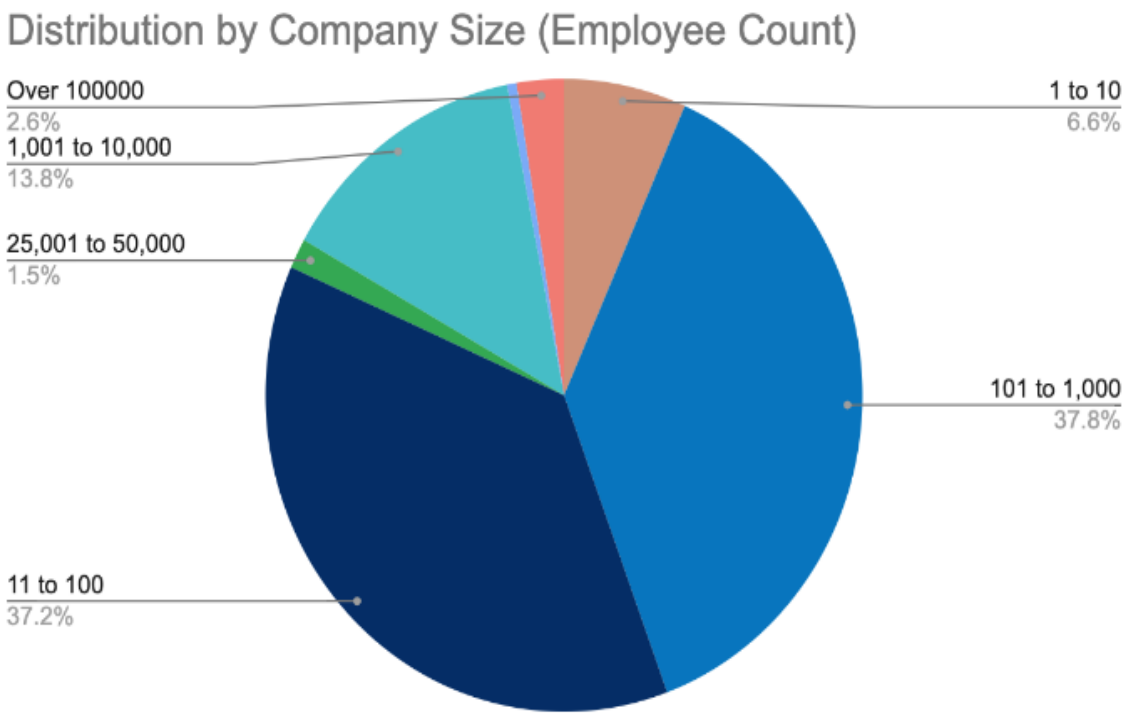
- Crime of Opportunity
  - IOT, Lack of Controls, Low Investment in Security
- Critical Infrastructure
  - Foodchain
- Ability for Systemic Impact

What we plan to cover today

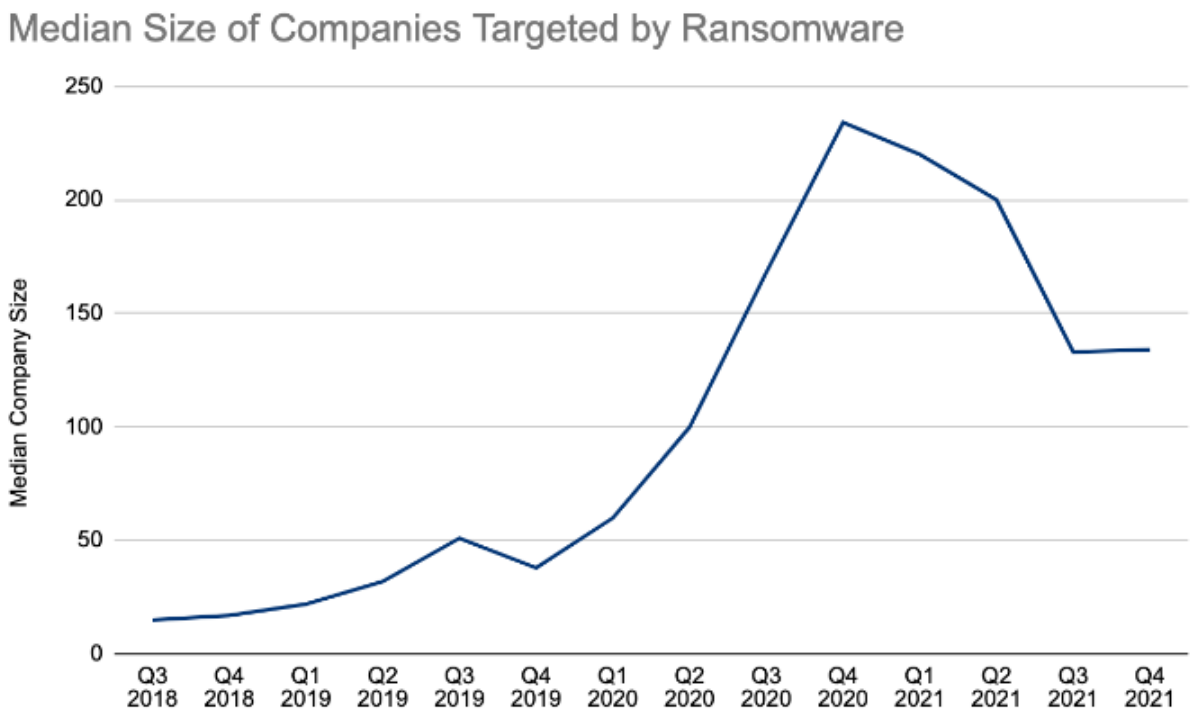
- Who is at Risk
- Understanding the Risk
- Cost of the Risk
- How Organizations can Prepare

WHO IS AT RISK?

Distribution by company size



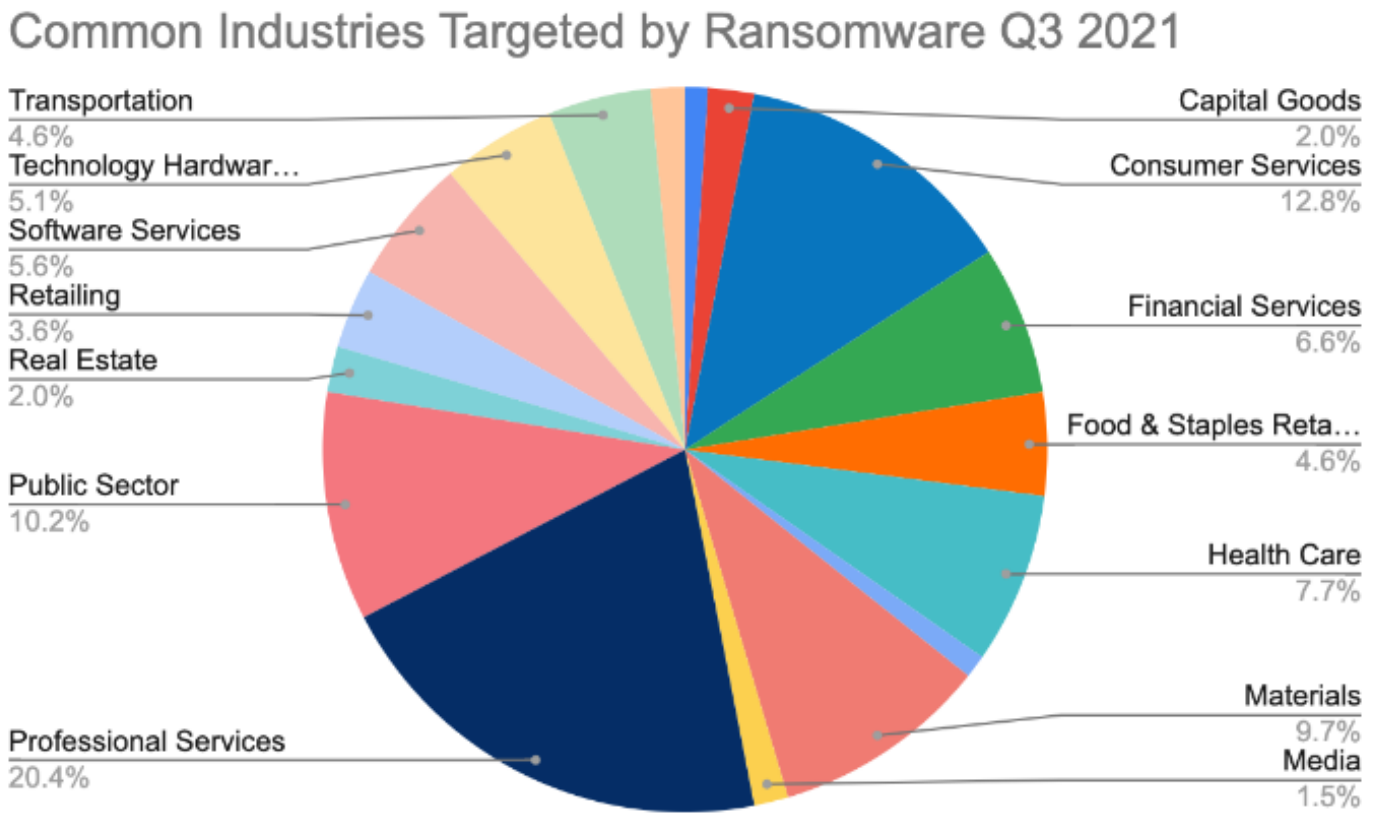
COVEWARE



COVEWARE

*"**Over 80% of attacks occur on companies with less than 1,000 employees.** These firms are much less likely to have the budget to implement the bare minimum protections necessary to keep them safe from ransomware attacks. More so than large enterprises, small businesses may outsource IT entirely to third party providers and inadvertently create a vulnerable entry point if the methods the vendor is using to manage the company are not airtight and routinely audited."*

Common Industries Targeted by Ransomware in Q3 2021



COVEWARE

UNDERSTANDING THE RISK

DEFINING YOUR RISK

Impact across the organization

Cyber is not just an IT issue

It is an enterprise risk that impacts many key stakeholders within your organization.

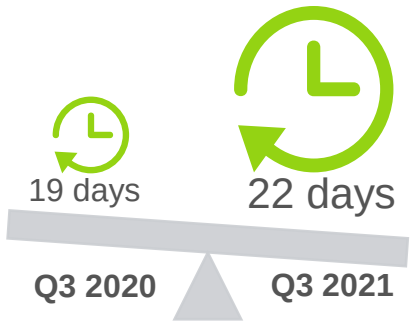
Cyber Trends

Dominated by ransomware, regulations & supply chain cyber risk

- Sources: Coveware Ransomware Blog & MMC Cyber Analytics Center

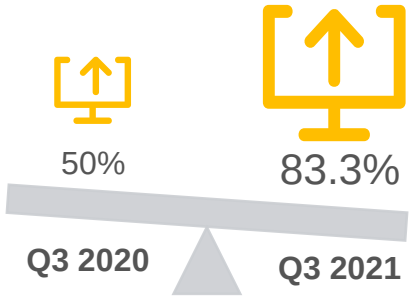
Ransomware attacks continue to increase in frequency, severity & sophistication – impacting orgs of all sizes & industries:

Average downtime:



~16% YOY increase

Cases with data exfiltration:



~66% YOY increase
3% increase vs. Q2 2021

2021 Ransom Headlines:

$8.3M average ransom payment
$11.9M average ransom demanded

- Large insurer: **$40M** paid
- Oil pipeline: **$4.4M** paid
- Infrastructure: **$50M** demanded
- Food manufacturer: **$11M** paid
- Chemical distribution: **$4.4M** paid
- Tech hardware: **$50M** demanded

Privacy regulations are intensifying and there's still a patchwork approach:

- **GDPR** fines are growing (~$27M BA, ~$24M Marriott, ~$41M H&M)
- **CCPA** (California Consumer Privacy Act) + similar legislation (i.e. VA CDPA) allow for private rights of action and require additional compliance efforts
- **BIPA** (IL Biometric Information Privacy Act) litigation is expensive and is on the rise with increased use of biometric identifiers, especially for employee access – driving additional underwriting questions

Supply chain and systemic risk garner more focus:

- **Aggregation** exposure a concern for underwriters
- **Systemic loss** – possible cyber risks:
  - Common vulnerabilities – in hardware or software
  - Common dependencies – vendors (such as cloud providers) and software
- **Cyber events** are driving increased scrutiny: SolarWinds, Accellion, Microsoft Exchange, Kaseya & Log4j

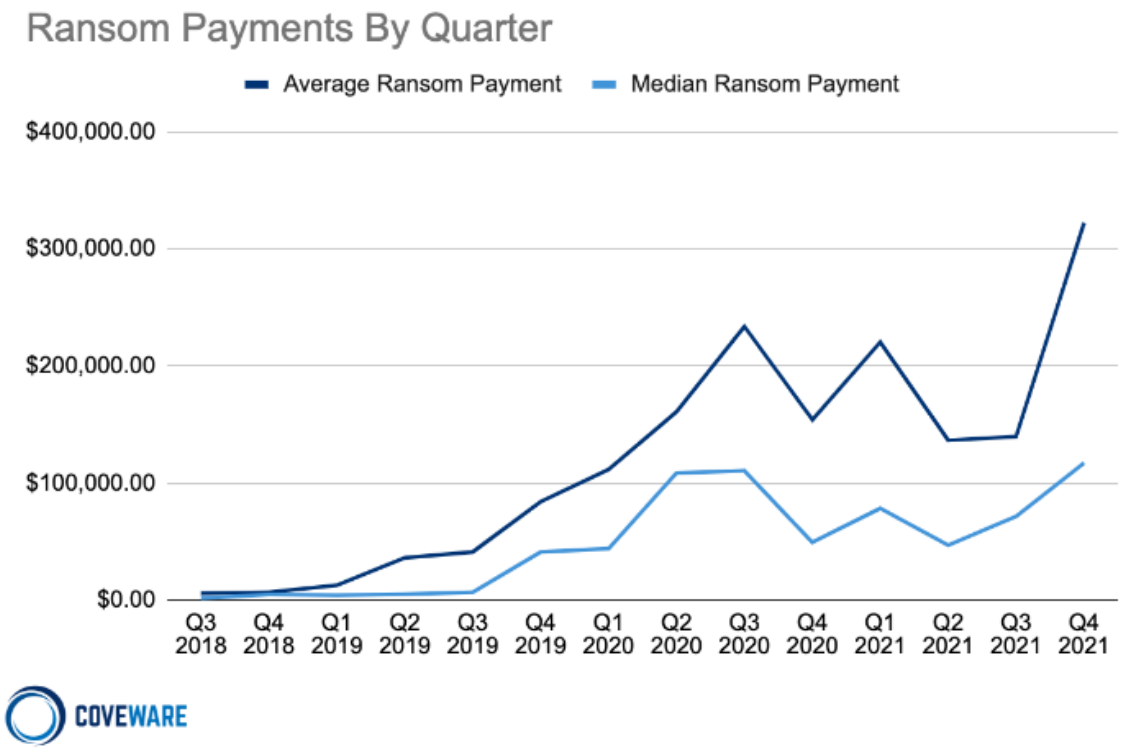
Cyber risk has THREE core stakeholders

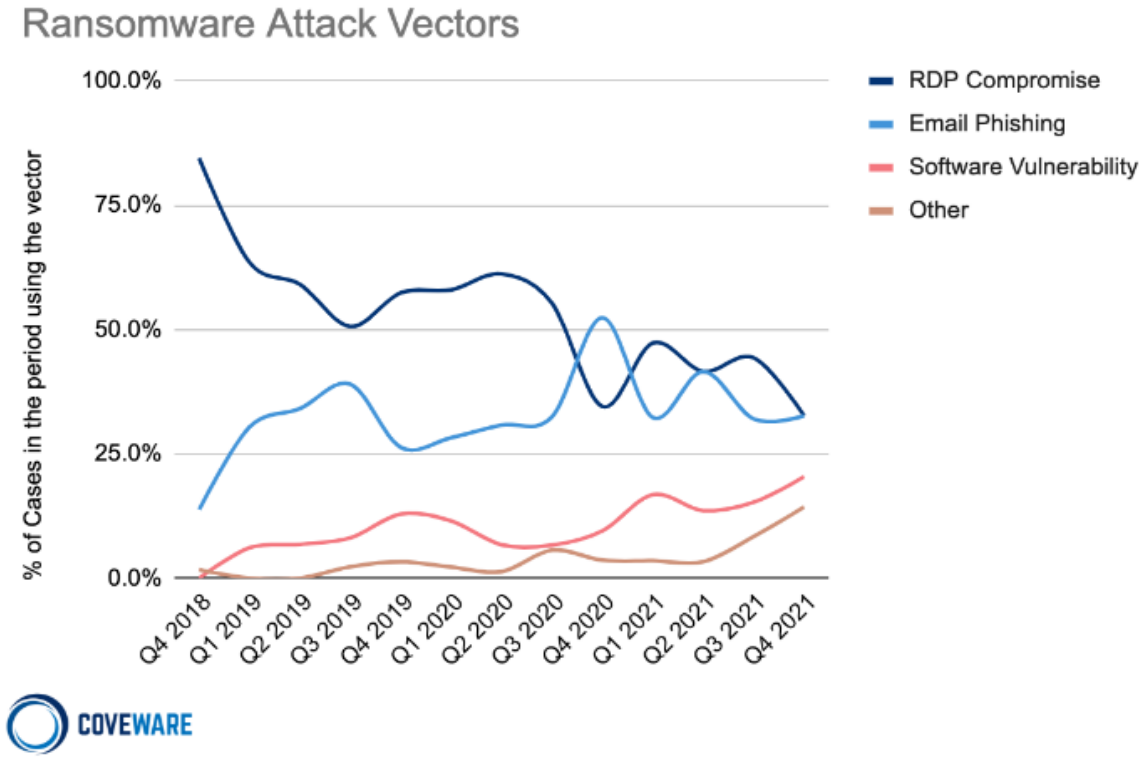
COSTS OF RISK

Quick Facts

- 2200 Cyberattacks per day Norton.com
- Data breach costs rose from $3.86 mil to $4.24 mil from 2020 to 2021 IBM
- Average cost of ransomware attack was $4.62 mil in 2021 IBM
- Cybercrime costs organization $1.79 mil every minute RiskIQ
- Cybercrime costs the world economy more than $6 trillion in 2021 Cybersecurityventures

Average Ransomware Payment & Attack Vector





“

What are Potential Costs & Liabilities

How does a stand-alone cyber policy protect your company?

First Party

Incident Response (Legal, Forensic, Notification)
Data Restoration / Recovery
Network Business Interruption
Contingent Business Interruption (i.e. IT & Supply Chain)
Cyber Extortion
Computer Hardware Restoration

Third Party

Network Security Liability
Privacy Liability
Privacy Regulatory Defense Costs & Penalties
Media Liability
PCI Fines/Penalties & Assessments

Loss or damage to reputation
Legal liability to others for computer security breaches
Extra expense to recover/respond to a computer attack
Legal liability to others for privacy breaches of confidential information
Loss of revenue due to a computer attack
Costs to investigate and notify others of a breach
Loss of damage to data/information
Regulatory actions, fines and scrutiny
Electronic & non-electronic media content
Cyber-terrorism
Cyber-extortion

Cyber tools & analytics overview

1

Cyber Self-Assessment - CORE

Maturity analysis on an organization's cybersecurity program based on user responses.

2

Ransomware Insights Report & Cost Model

Regression analysis of known ransomware event losses to derive average cost and ransom demand for your organization.

3

Business Interruption Loss Modeling

A stochastic model that gives an indication of the business income loss by looking at multiple scenarios.

4

Privacy Breach Loss Modeling

A privacy breach model that provides potential loss scenarios based on clients records, industry and size.

5

Benchmarking

Insights into the buying behaviors and changes in price for firms similar in size and industry.

6

Cyber Threat Model – Bitsight & Security Scorecard

Data breach probability based on the external perceptions of your firm's operational footprint and technical vulnerabilities.

PREPARING YOUR ORGANIZATION

Cyber Preventative Measures

1. Establish / support VPN or other secure connectivity solutions to employee workstations and mobile devices via MDM.
2. Ensure multi-factor authentication (MFA) across critical systems
3. Back up & test system resiliency
4. External perimeter protections / Log and monitor access
5. Maintain clear inventories of digital assets and locations
6. Email controls - filters and sandboxing; strong passwords; frequent resets
7. Consistent employee awareness training
8. Verify requests for information

Cyber Preventative Measures

9. Encrypt whenever possible
10. Have written procedures in place to handle sensitive place
11. Be conscious of privacy issues with contact tracing and scanning of business invitees.
12. Schedule a third-party assessment and vulnerability scan of your network
13. Ensure updated patching of systems, browsers, software, anti-virus
14. Ready your incident response plan - Review MSA's of incident response firms such as legal and forensic firms that are approved by your cyber insurance carrier.
15. Consider cyber insurance in connection with your incident response plan
16. Segment your network
17. Contractual controls and audit

Vendors: The Weak Cyber Link?

Challenge: **Reliance on vendors is increasing** – and cyber events are increasing in frequency and severity. Companies are struggling to manage what they can't control: vendors.

Leverage vendors as a weak cyber link to drive a broader discussion on Cyber Risk:

1. Staying abreast of vendor cybersecurity controls and vulnerabilities
2. Managing vendor cyber risk through contracting practices
3. Quantifying the potential impact of a vendor cyber incident
4. Managing vendor risk comprehensively and cross-functionally

- This applies to ALL vendors, not just technology vendors!
- We help companies understand their vendor weak links, quantify the vendor risk, and manage it via insurance & consulting!

Favors Buyer Neutral Favors Insurers

Cyber Insurance Market Snapshot

Claims & Rates	Structure & Coverage	Underwriting
		
Claims frequency and severity remains high driven by ransomware. Ransomware, systemic risk & regulations continue to drive concern. Losses have accelerated pricing pressure even on loss free accounts with good controls. Excess pricing is increasing faster than primary, compounding increases. Expect increases to continue into 2022.	Insurers are aggressively managing global capacity & increasing SIRs. Distressed classes & large towers may see capacity challenges. Some insurers imposing more restrictive coverage on ransomware, contingent business interruption (systemic risk), regulatory cover (biometric information), etc.	Full application & responses to ransomware Q's are required; carriers using 3rd parties to externally scan environments. Also expect inquiries on recent supply chain events including Log4j, biometric info, & operational technology.
November Cyber Premiums: **+123%** Avg increase same limits **+186%** Avg increase all renewals* **All renewals include limits changes.*	**November Cyber Renewals:** **39%** reduced limits **7%** increased limits **66%** increased SIRs *Driven by insureds minimizing increases & less available capacity.*	**12** Key Controls & Best Practices are now viewed by carriers as essential

*For discussion and general information purposes only. Specific coverage details may vary.

Insurance Coverage Gap Analysis

Privacy & Cyber Perils	Property	General Liability	Fidelity Bond	Computer Crime	E&O	Special Risk (KRE)	Broad Privacy & Cyber Policy
Destruction, corruption or theft of your electronic information assets/data due to failure of computer or network.	Becoming less available						Information asset protection
Theft of computer system resources.	Becoming less available						Information asset protection / crypto-jacking - sublimit
Business Interruption due to a material interruption in an element of your computer system due to failure of computer or network security (including extra expense and forensic expenses).	Becoming less available						Network Business Interruption
Business interruption due to your service provider suffering an outage as a result of their security failure or system failure	Becoming less available						Network Business Interruption (sublimitted or expanded based upon risk profile)
Indemnification of your notification costs, including credit monitoring.							Privacy Liability
Defense of regulatory action due to a breach of privacy regulation.							Privacy Liability
Coverage of Fines and Penalties due to a breach of privacy regulation.							Privacy Liability (where insurable by law)
Social Engineering Fraud							Cyber-Crime

Not Covered Covered Dependent upon specifics of claims, may not be covered

10 Security/Privacy Risk Controls Requested by Leading Cyber Insurance Carriers* (Q2 2021)

1. Multi-factor authentication (MFA) (remote access, admin access, email, critical systems, vendor access, etc.)
2. A current and tested incident response plan
3. No open ports for remote access (e.g., Remote Desktop Protocol [RDP])
4. Air-gapped and encrypted backups, including the demonstrated ability to test and restore from backups
5. The sunsetting or removal of end-of-life software
6. The presence of an advanced endpoint detection and response (EDR) solution
7. Enabled logging for all systems, software, and perimeter devices
8. Employee awareness trainings and phishing simulations
9. An updated patch management program
10. A password manager/vault and adoption of least privilege access

**Importance & weight varies by industry class, exposure base (revenue, # of records), etc.*

QUESTIONS + THANK YOU!

Dan Hanson

+1 763 548 8599

Dan.Hanson@MarshMMA.com

GEAPS EXCHANGE
KANSAS CITY • 2022

We want your feedback!

Download the "*GEAPS Exchange*" app to take the session survey.

Share on Social!

#GEAPSExchange

Wifi Network: GEAPS2022 Password: Exchange92

GEAPS EXCHANGE KANSAS CITY • 2022