Cyber Attacks: Are you at Risk?

JKJ | JOHNSON KENDALL JOHNSON

Speaker Info

JKJ | JOHNSON KENDALL JOHNSON

Insurance & Risk Management Brokerage

- Property/Casualty, Benefits, Financial Services
- Serving over 225 senior living communities across 22 states
- 60 years of Experience

Rafael Haciski, Esq
Risk Management and Insurance Advisor

Speaker Info

Alexandra H. Bretschneider, CCIC
Cyber Practice Leader, Account Executive

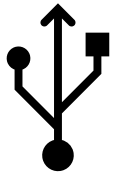
- IT Consulting Background
- *Cyber COPE Insurance Certification* from Carnegie Mellon Heinz College of Information Systems & Public Policy

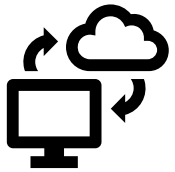
JKJ Cyber Practice

- 2021 - JKJ is proudly recognized as ***the top broker internationally for Cyber Insurance*** by Advisen, a leading provider of data, technology, events, and media for insurance professionals.

Cyber Incident - What are we talking about?

- Ransomware
- Phishing Attack
- Data Breach
- Denial of Service Attack
- Lost or Stolen Device/Files
- Disclosure of Private Information
- Hacking
- Malware
- Vendor Error or Negligence
- Physical Security Breach
- The Unknown…



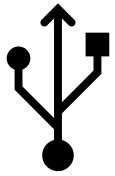


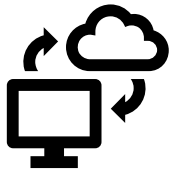
- It is estimated more than 50 billion devices and processes are connected to the internet

- Cybercrime is projected to cost the world $6 trillion in 2021, *making it the third-largest economy after the U.S. and China.*

Cyber Incident - What are we talking about?

- Ransomware
- Phishing Attack
- Data Breach
- Denial of Service Attack
- Lost or Stolen Device/Files
- Disclosure of Private Information
- Hacking
- Malware
- Vendor Error or Negligence
- Physical Security Breach
- The Unknown…



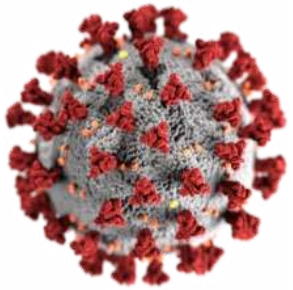


- It is estimated more than 50 billion devices and processes are connected to the internet

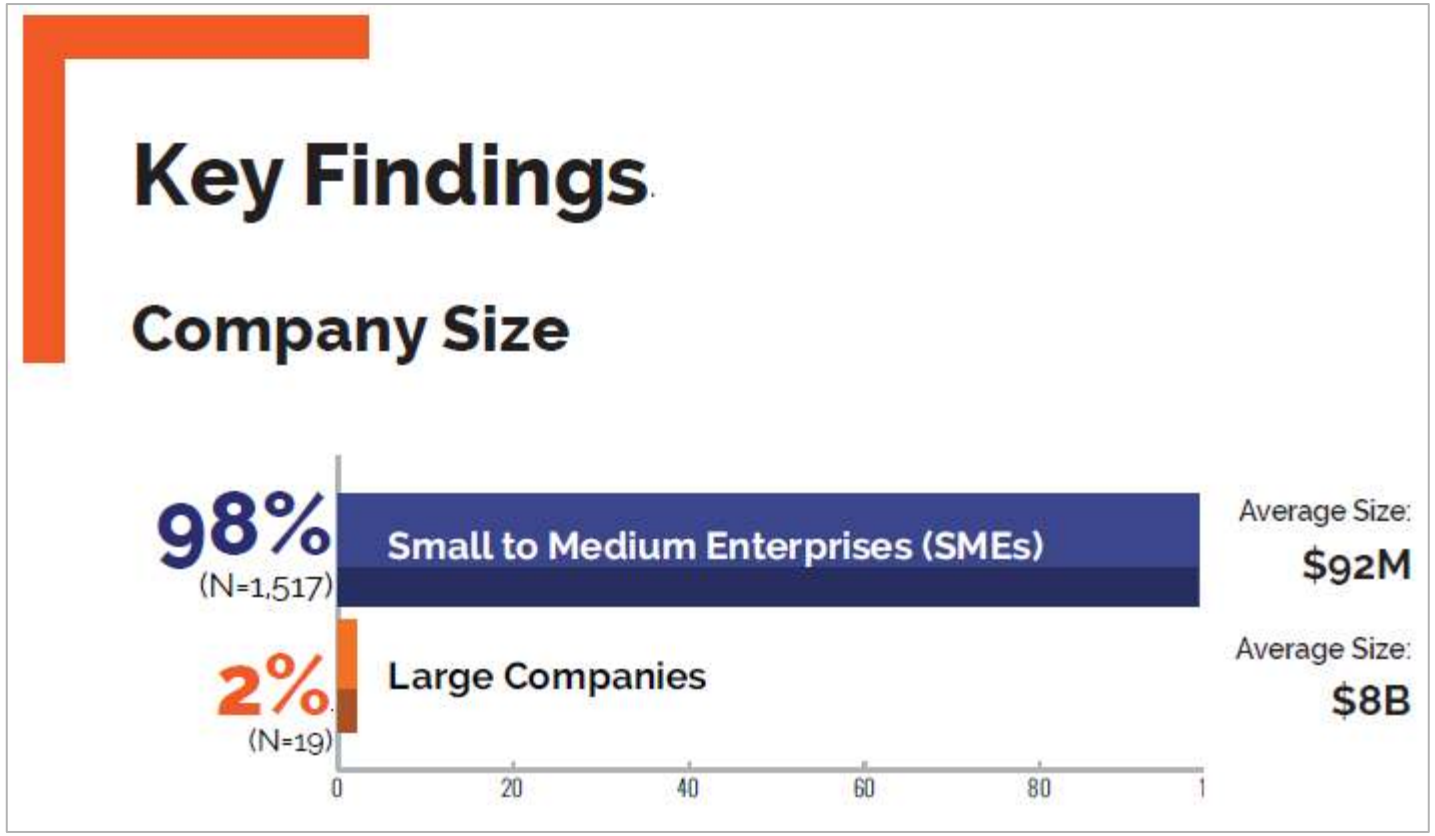
- Cybercrime is projected to cost the world $6 trillion in 2021, *making it the third-largest economy after the U.S. and China.*

CYBER CLAIM TRENDS

Data Breaches → **Social Engineering** → **Ransomware**



Who is being targeted?



This year's report continues a painful trend as it starts to hit the mathematical extremes of the prior studies. The attacker's shift in preference to small and mid-sized organizations has become overwhelming, where the data shows that being an organization of specific size is more dangerous than being in a specific industry. The only universal constant across both large and small organizations is that incident costs continue to increase and actually appear to be accelerating.

Daimon Geopfert
National Leader,
Security and Privacy Services
RSM US

Source: NETDILIGENCE® CYBER CLAIMS STUDY 2020 REPORT

Small to Medium Enterprise (SME)

Categorized in this study as organizations with less than $2 billion in annual revenue.

Ransomware by the numbers…

- ***In 2020, average extortion demand skyrocketed to $178,254 and attacks cost over $1 billion in damages.***
- ***In 2020, 55% of attacks were on small businesses with less than 100 employees.***
- ***In 2020, the average business experienced 16 days of interruption.***
- ***In 2021, a business will be hit by ransomware every 11 seconds.***
- ***In 2021, ransomware will cost businesses $20 billion.***

In the news….2020-2021

GBMC Nurse: Hospital 'Crippled' By Ransomware Cyberattack

By Paul Gessler December 18, 2020 at 10:55 pm **Filed Under:** Baltimore, Baltimore News, GBMC, Local TV, Maryland News, ransomware cyberattack, Talkers

UPDATE: UHS Health System Confirms All US Sites Affected by Ransomware Attack

In an Oct. 3 update, the UHS health system confirms all US sites were impacted by the ransomware attack that struck more than a week ago; phishing incidents and more ransomware attacks complete this week's breach roundup.

$5 Million settlement in hospital data breach

Blackbaud Confirms Hackers Stole Some SSNs, as Lawsuits Increase

An SEC filing reveals hackers gained access to more unencrypted data than previously thought. Some of the millions of breach victims have filed lawsuits against the vendor in response.

Woman dies during a ransomware attack on a German hospital

It could be the first death directly linked to a cybersecurity attack

Cyber Insurance was designed to respond to these situations!

In the news….2020-2021 *(continued)*

Supply Chain Risk is an emerging threat

FINANCIAL

Top insurer CNA disconnects systems after cyberattack

Cybercrime

Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack

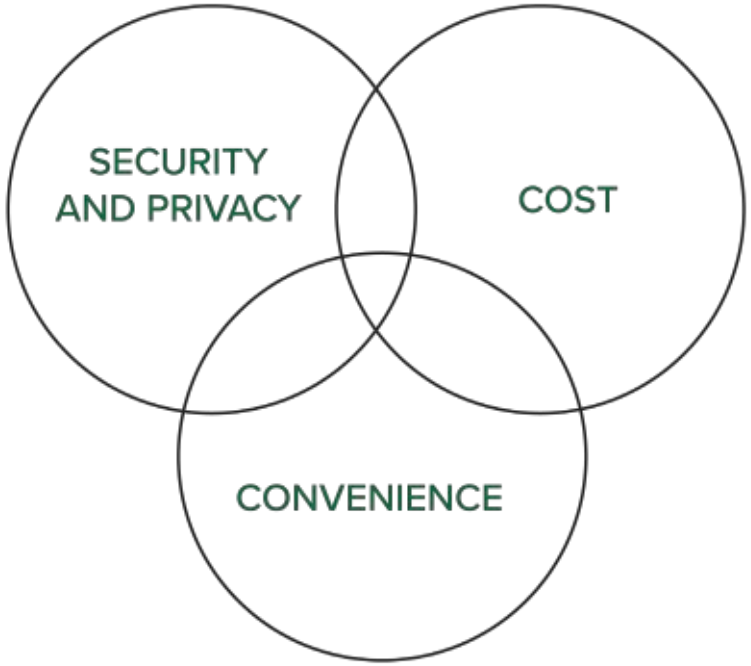
The company's CEO authorized the payment as a means to restart the pipeline's systems quickly and safely

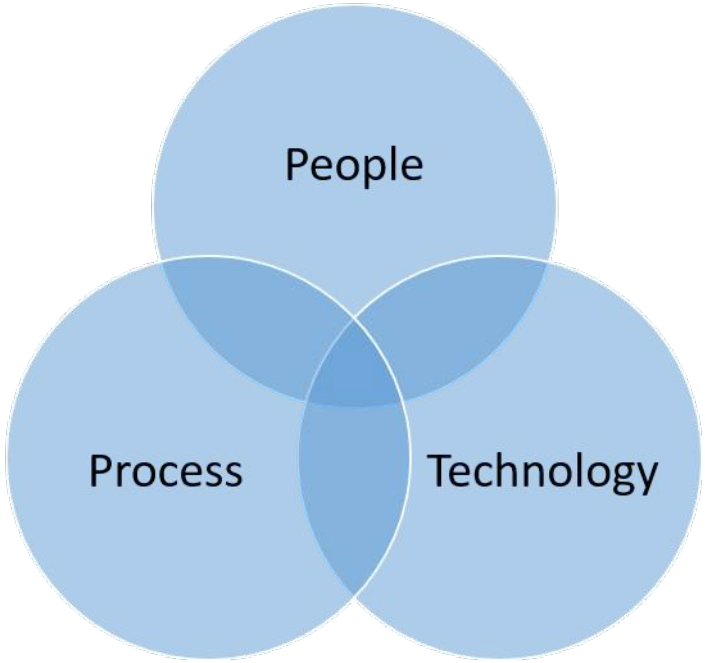
Everything you need to know about the Microsoft Exchange Server hack

Updated: Vulnerabilities are being exploited by Hafnium. Other cyberattackers are following suit.

SolarWinds breach exposes hybrid multicloud security weaknesses

Cyber Risk Management





GOALS:

1. Reach a state of ***CYBER RESILIENCE*** in which you can properly identify, respond, and recover from a Cyber Incident.

2. Be cognizant of the ***REASONABLENESS STANDARD.***
    - What would I reasonably expect of a similar company?

Cyber Risk Management

New Consideration:
Supply Chain Risk – Vendor Management

- Inventory of Vendors
  - What do they have access to? (System and/or information)
  - How is access controlled?

- What do the contracts say?
  - Indemnification, Hold Harmless, Confidentiality, Responsibility
  - Insurance requirements

What is Cyber Insurance

Cyber Insurance covers the economic or legal costs arising out of a Data Disclosure or Network event.

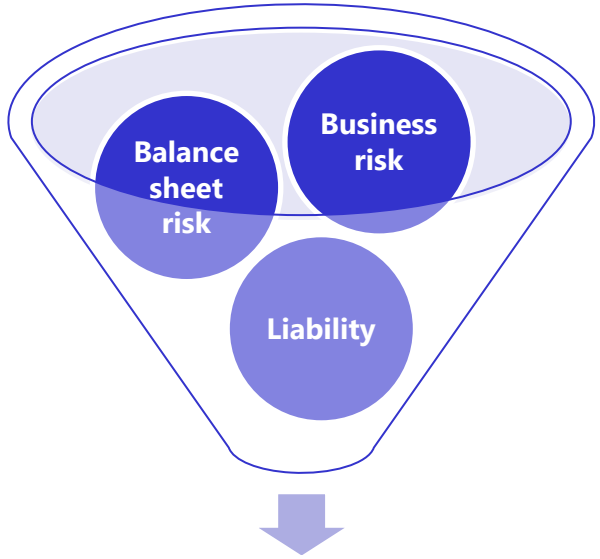
- Offers both services & financial risk transfer.

INCIDENT RESPONSE: To determine what happened, how to repair the damage, to reduce downtime and to meet privacy regulatory requirements. Includes IT Forensics, Legal, PR, and notification costs.

LAWSUITS & PRIVACY REGULATORY INVESTIGATIONS: Legal fees, legal settlements and also regulatory fines where insurable (such as HIPAA, PCI, GDPR, CCPA, etc violations)

CYBER CRIME: Costs such as ransom or extortion payments, phishing, and social engineering.

BUSINESS LOSSES: Impact to operations or ability to generate revenue both during an incident and afterward as it impacts your reputation.



Cyber Insurance – Key Considerations

1) Adequacy of Limits
2) Hosted vs. On Premise Services
3) Reputational Harm
4) Bodily Injury or Property Damage
5) Social Engineering
6) Evolving Regulations

2021 STATE OF THE MARKET

- **Significant Rate Increases**

Ransomware attacks increase by 170%, drive cyber insurance rates

July 07, 2021

Ransomware attacks driving cyber reinsurance rates up 40%

Willis Re International told Reuters that recent high-profile ransomware attacks are sending reinsurance rates soaring.

By Jonathan Greig | July 2, 2021 -- 20:33 GMT (13:33 PDT) | Topic: Security

Global cyber insurance pricing increases 32%: Howden

Luke Harrison 05 July 2021

Cyber industry loss ratio at record-high 67% in 2020: Aon

21st June 2021 - Author: Matt Sheehan

2021 STATE OF THE MARKET

- **Coverage Changes / Limitations**
  - Reduction in limits on Business Interruption & Dependent Business Interruption
  - Social Engineering/Crime
  - Limitations or Coinsurance on Extortion Coverage
  - Specific Event Exclusions – SolarWinds Orion Software, MS Exchange Server

- **Insurance Carrier Requirements**
  - Multi-Factor Authentication
  - Secured Remote Connectivity – No Public RDP
  - Segregated Backups
  - Employee Training
  - Cyber Incident Response Policy
  - EDR / IDS and NextGen Antivirus tools deployed
  - Pen Testing/ Vulnerability Assessments
  - Identifying key IT and non-IT vendors