Cyber Liability in Senior Living:

Top 5 Best Practices & Risk Management Strategies for LTC Providers

JKJ | JOHNSON KENDALL JOHNSON

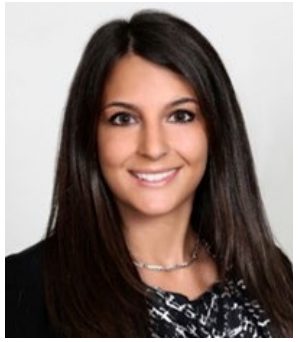
Speaker Info

JKJ | JOHNSON KENDALL JOHNSON

Insurance & Risk Management Brokerage

- Property/Casualty, Benefits, Financial Services
- Headquartered Newtown, PA
- Independently-Owned
- 60 years of Experience
- Serving over 225 senior living communities across 20+ states

Speaker Info



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

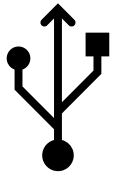
- IT Consulting Background
- *Cyber COPE Insurance Certification* from Carnegie Mellon Heinz College of Information Systems & Public Policy

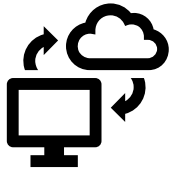
JKJ Cyber Practice

- 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…



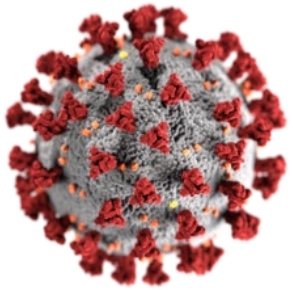


- It is estimated more than 50 billion devices and processes are connected to the internet

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

CYBER CLAIM TRENDS

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



Who is being targeted?

Key Findings

Company Size

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.*
  - *55% of attacks were on small businesses with less than 100 employees.*
  - *The average business experienced 16 days of interruption.*
- ***In 2021***
  - *Average extortion demand increased to $570k*
  - *A business will be hit by ransomware every 11 seconds.*
  - *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

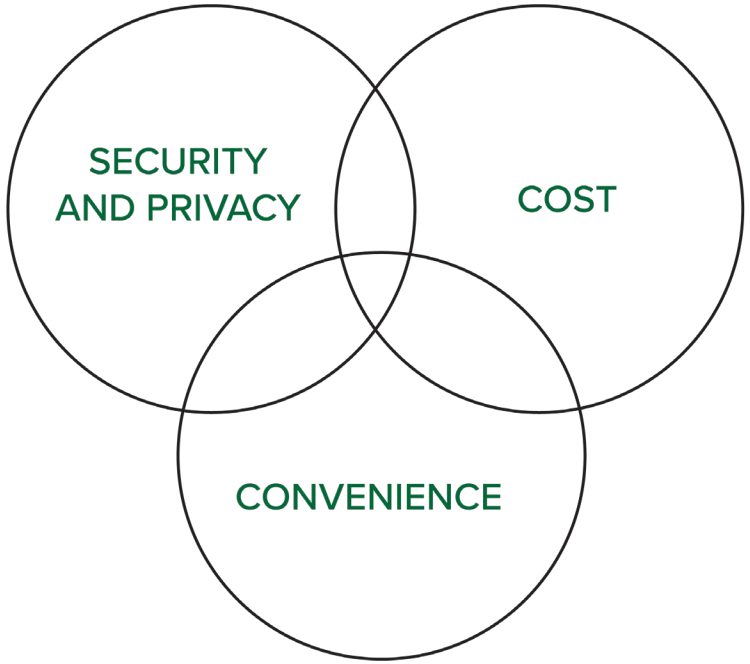
SUPPLY CHAIN ATTACK —

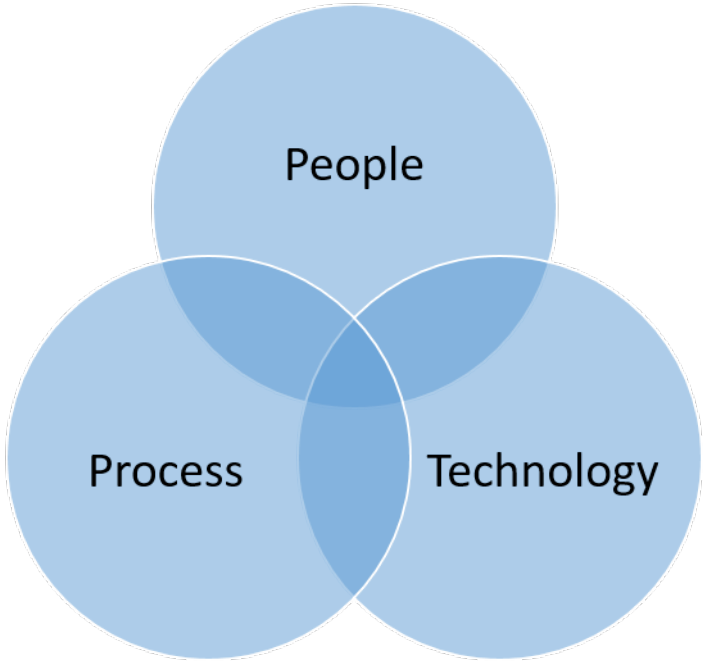
Up to 1,500 businesses infected in one of the worst ransomware attacks ever

Mass compromise is having cascading effects around the world.

DAN GOODIN - 7/6/2021, 4:48 PM

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
IT and Non-IT vendors

- 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 IS ONE PIECE OF YOUR CYBER RISK MANAGEMENT STRATEGY

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

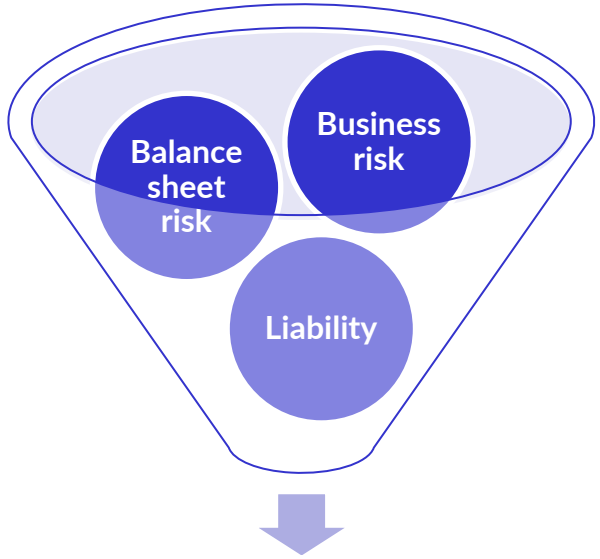
- Offers both services & financial risk transfer.

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)

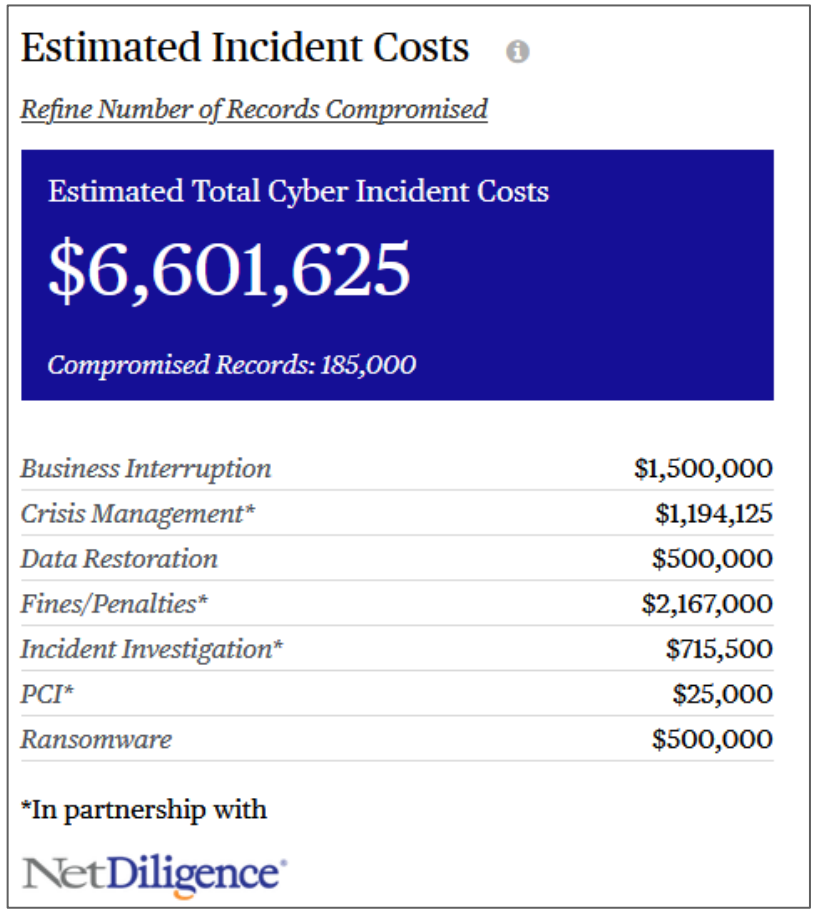
CYBER CRIME: Costs such as ransom or extortion payments, phishing, and social engineering.

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) Hardware Coverage & Betterment
7) Evolving Regulations



Estimated Incident Costs

Refine Number of Records Compromised

Estimated Total Cyber Incident Costs

$6,601,625

Compromised Records: 185,000

Business Interruption	$1,500,000
*Crisis Management**	$1,194,125
Data Restoration	$500,000
*Fines/Penalties**	$2,167,000
*Incident Investigation**	$715,500
*PCI**	$25,000
Ransomware	$500,000

*In partnership with

NetDiligence

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

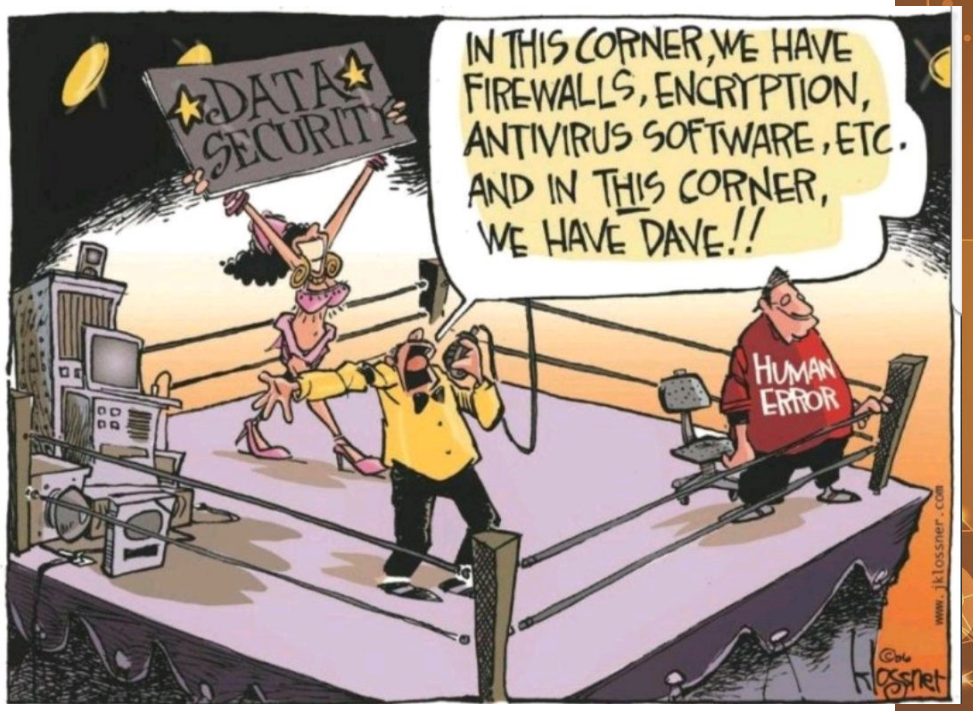
2021 STATE OF THE MARKET

- **EVOLVING REGULATIONS – ESPECIALLY AROUND RANSOMWARE**
- **INSURANCE 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
- **INSURABILITY 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
  - Patch Management
  - Penetration Testing/ Vulnerability Assessments
  - Identifying key IT and non-IT vendors

BONUS: *JKJ and your Cyber Insurance carrier have resources to assist in these areas.*

5 Best Practices to be Prepared

1) PREPARE TO MEET INSURABILITY REQUIREMENTS
2) MANAGE ACCESS AND PATCHES
3) EMPLOYEE TRAINING
4) REVIEW YOUR INSURANCE COVERAGE
5) INCIDENT RESPONSE PREPAREDNESS
   - Test your backups
   - Tabletop your policy & procedures



BONUS: *Review your financial transaction & change authorization procedures.*

SAMPLE COVERAGE COMPARISON

	CFC (Lloyds of London)	Tokio Marine (Houston Casualty)	At Bay (HSB Specialty Insurance)
AM Best Rating	A, XIII	A++, XV	A++, X
First Party Coverages			
Incident/Breach Response	$2,000,000 $0 deductible Defense outside the limit	$2,000,000 Separate limit of insurance not subject to policy aggregate	$2,000,000 Additional $1M limit outside the aggregate
Legal & Regulatory Costs	$2,000,000	$2,000,000	$2,000,000
IT Security & Forensic Costs	$2,000,000	Part of Incident/Breach response	Part of Incident/Breach response
Crisis Communication	$2,000,000		
Privacy Breach Management Costs	$2,000,000		
Post Breach Remediation Costs	$50,000 subject to a max of 10% of all sums paid from a cyber event; $0 deductible	$25,000	See Betterment
Funds Transfer Fraud / Social Engineering	$1,000,000	$500,000	$250,000
Theft of Funds Held in Escrow	$1,000,000	$500,000	$250,000
Theft of Personal Funds	$1,000,000	Not included	Not included
Extortion	$2,000,000	$2,000,000	$2,000,000
Corporate Identity Theft	$1,000,000	Not included	Not included
Telephone Hacking	$1,000,000	$500,000	$2,000,000
Push Payment Fraud/Invoice Manipulation	$50,000	$250,000	$1,000,000
Unauthorized Use of Computer Resources	$1,000,000	$500,000	$2,000,000
System Damage and Rectification	$2,000,000	$2,000,000	$2,000,000
Income Loss and Extra Expense	$2,000,000		$2,000,000
Additional Extra Expense	$100,000	Not included	Not included
Dependent Business Interruption	$2,000,000	$2,000,000 UPDATED	$2,000,000
Reputational Harm	$2,000,000	$2,000,000	$2,000,000
Claim Preparation Costs	$25,000 $0 deductible	Not included	Included
Hardware Replacement Costs	$2,000,000 Broad; not limited to bricking	$2,000,000 Limited to bricking	$2,000,000 Limited to bricking

SAMPLE COVERAGE COMPARISON

	CFC (Lloyds of London)	Tokio Marine (Houston Casualty)	At Bay (HSB Specialty Insurance)
Third Party Liability Coverages			
Network Security Liability	$2,000,000	$2,000,000	$2,000,000
Privacy Liability	$2,000,000		$2,000,000
Management Liability	$2,000,000	Not included	Not included
Regulatory Fines	$2,000,000	$2,000,000	$2,000,000
PCI Fines & Penalties	$2,000,000	$2,000,000	$2,000,000
Media Liability (Defamation, IP Infringement)	$2,000,000	$2,000,000	$2,000,000
Enhancements			
Court Attendance Costs	$100,000 *$0 deductible*	$25,000 *$0 deductible*	Not included
Contingent Bodily Injury	$250,000	$250,000	$250,000
Corrective Action Plan Costs	$50,000	Not included	$25,000
Betterment	Not included	Not included	$25,000
Property Damage	Not included	$50,000	Not included
TCPA Defense Coverage	Excluded	$50,000	Excluded
Reward Expense	Not included	$50,000	Included
Voluntary Notification	Not included	Not included	$100,000
Voluntary Shutdown	Included	Included	Included
Hammer Clause	80/20	70/30	90/10
Retroactive Date	Full prior acts	Full prior acts	Full prior acts
Deductible	$35,000	$25,000	$25,000
Aggregate Deductible	N/A	$75,000	N/A
Waiting Period	6 hours	8 Hours (12 hours for Dependent System)	8 hours
Indemnity Period (Business Income)	12 months	6 months (4 months for Dependent System)	6 months
Indemnity Period (Reputational Harm)	12 months	6 months	6 months
Premium	**$33,158**	**$13,465**	**$16,959**

OPEN Q&A

Thank you!