CYBER RISK MANAGEMENT CAPABILITIES

2023

johnson kendall johnson

Contents

JKJ OVERVIEW

Johnson Kendall & Johnson (JKJ) is an independently owned insurance brokerage and risk management firm based just outside of Philadelphia in Newtown, Pennsylvania. Since 1959 the firm has been serving the corporate and personal insurance marketplace. JKJ proudly serves clients in 46 states and throughout the world. JKJ is proudly considered the "founders" of the 401k plan – establishing the first 401k ever created which remains intact today!

JKJ's mission is summed up best by saying, "**Our Passion Is Your Protection**." We pride ourselves in our desire to become a trusted resource for our clients' business decisions. Formerly, JKJ was part of a larger organization, The Johnson Companies, which sold to Noble Lowndes in 1992. However, the Property and Casualty division, JKJ, Inc., remained independent. At the commencement of the restructuring in 1992, JKJ made several commitments that still hold true today:

I. The needs of clients will be top priority and guide all decision-making processes
II. JKJ would grow organically rather than making acquisitions or being acquired
III. Continually develop state-of-the-art Safety and Claims management services, exclusive of insurance company involvement
IV. Attract, develop and retain the best employees to deliver on our mission of exceptional service to our clients
V. Develop a long-term succession and perpetuation plan in the form of mentoring and employee ownership – ever JKJ associate is an owner via the Employee Stock Ownership program put into place over forty years ago
VI. Foster an environment of diversity and inclusion
VII. Promote a culture of philanthropy through community engagement

Through the efforts of professionals with focused experience in underwriting, claims management and safety management, and the enhancements afforded by our investment in technology, we devise and deliver unique service programs that will address the practical Insurance & Risk Management needs of our clients, their employees, and residents. Our interactive approach coupled with technical expertise will enable Risk Management improvement and a reduction of long-term insurance costs.

JKJ's personalized service is the reason why clients benefit from our approach to protection, which includes loss control and risk management services. Our clients range from Fortune 1000 companies to sole proprietorships in fields as wide-ranging as biotechnology and hospitality to healthcare and real estate developers. JKJ believes in taking a consultative role with our clients by partnering in their Insurance and Risk Management Program.

An important role for JKJ is not just to solve problems -- it is to prevent them. One way we prevent them is by education. By educating our clients, we enable them to secure and maximize their assets and to utilize them with peace of mind.

While the broader brokerage community continues to consolidate at record breaking numbers, JKJ has remained focused entirely on its clients, people, and the community. We are proud to be a Certified Evergreen company, committed to remaining independent and pursuing innovation. We became members of the Tugboat Institute which is an organization committed to support Evergreen leaders.

CYBER PRACTICE

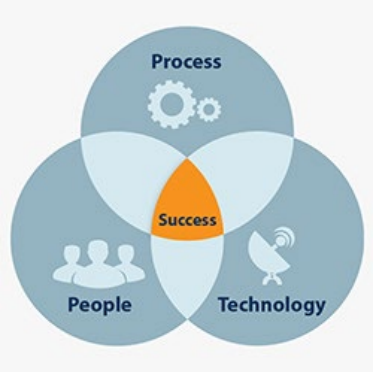
With the pervasive use of technology in business operations, Cyber has quickly risen in the ranks of greatest threats facing businesses across all industries today. JKJ has established itself as a premier cyber insurance brokerage and thought leader. ***In 2021, JKJ is proudly recognized as the top broker internationally for Cyber Insurance*** by Advisen, a leading provider of data, technology, events, and media for insurance professionals. JKJ has again been nominated for this distinguished award in 2022 and 2023!

Through our dedication to knowledge and experience in cyber liability, we educate our clients on the latest claim trends, changes in insurance terms, and risk management strategies. JKJ had the foresight that Cyber would become one of the greatest risks facing businesses, naming a former IT consultant as Cyber Practice Leader in 2020 – Alexandra Bretschneider. Alexandra is one-of-less-than-200 individuals worldwide to have obtained the Cyber COPE Insurance Certification (CCIC) designation from Carnegie Mellon – Heinz College of Information Systems and Public Policy.

JKJ's Cyber Practice develops content and delivers presentations to leading national healthcare associations, publishes white papers, conducts tabletop exercises, facilitates contract reviews, and develops a service model around education and deployment of cybersecurity best practices. JKJ continually educates its clients on the importance of cyber incident response, but also incident prevention strategies. We pride ourselves in placing business with the most reputable cyber insurance carriers and developing strategic partnerships with top legal, forensic, and cybersecurity service providers. Our cyber practice is relied upon by other accounting, legal, and cybersecurity firms for their clients in the areas of cyber insurance expertise and coverage reviews.

A "cyber incident" can take many shapes, including a Phishing or Social Engineering attack, Ransomware/Extortion event, Denial of Service attack, a Hacking attempt aimed at obtaining private or confidential information,

etc. The cost of global cybercrime is estimated to be over $400 billion annually. As the risks increase in pervasiveness, so does the Government regulation. With privacy laws passed in all 50 states (each different in their own right), in addition to several international laws, compliance is critically important.



A comprehensive Cyber Risk Management Program will include many parts, across people, processes, and technology. One key component of Cyber Risk Management is the procurement of a CYBER INSURANCE policy. JKJ's Cyber Practice includes developing expertise in the varied landscape of cyber insurance product offerings JKJ focuses on understanding the vast cyber insurance product offerings, the nuances of the various coverages as well as the pre and post-breach services offered. JKJ has established relationships with the top tier insurance carriers in the marketplace, both domestically and from Lloyds of London. JKJ developed a proprietary cyber insurance program designed specifically for our Healthcare clients to address their unique exposures. JKJ assists its clients in creating Cyber Incident Response programs to better prepare them for the suspected or actual incident.

JKJ is a member of TechAssure. TechAssure is global network comprised of carefully selected brokerages that specialize in risk management for clients that create, manufacture, sell or service technology-based products or services all over the world. As a TechAssure member, JKJ is able to provide exclusive benchmarking data, including coverage & cost information.

Through this membership JKJ affords our clients unique access to the most robust cyber risk management platform available: the NetDiligence eRiskHub. Through this hub and a variety of relationships with firms focused on PRE and POST breach services, JKJ can assist with the risk management strategies identified within this document.

JKJ has partnered with law firms who are respected as the top class of Privacy attorneys in the country (including Mullen Coughlin and Cipriani & Werner) and IT consultants who specializing in preventing and managing Cyber risk. JKJ hired a specialist with a background in IT Consulting in 2015, Alexandra Bretschneider, who leads the Cyber Practice today. After starting her career in the IT Advisory practice at Ernst & Young, she went on to pass the Certified Information Systems Auditor (CISA) exam and recently obtained the newly designed Cyber COPE Insurance Certification (CCIC) through Carnegie Mellon University.

JKJ Cyber Risk Management Services

Our team of experienced professionals has a deep understanding of the ever-changing cyber threat landscape and can help your organization stay ahead of the curve. We are excited to share a new bundle of Cyber Risk Management Services that are available to our clients!

Cybersecurity Controls Review/Insurability Analysis

JKJ's Cyber Practice will conduct a high level assessment by reviewing a questionnaire outlining the critical cybersecurity controls from the insurance perspective with you and your IT team (in-house or outsourced) and identify opportunities for improvement. JKJ will outline the impact of these controls on the insurance program in terms of their ability to influence pricing, terms and conditions. JKJ will help your organization create a roadmap towards improved cybersecurity and cyber risk management posture.

IRP Review & Tabletop Exercise

Insurance carrier applications often ask whether your organization has a Cyber-specific Incident Response Plan (IRP) in place. JKJ has templates we can provide to help your organization build an IRP; but more importantly, once you build it, you should put it to the test! JKJ will engage a privacy attorney, and IT Forensics firm, who are pre-approved/on panel with your insurance carrier to conduct a tabletop exercise of your IRP with various mock cyber incident scenarios. These exercises are best performed with the engagement of your IT, Operations, and Executive leadership teams. Sample incidents may include mock ransomware attacks or business email compromises. The time spent in these preparatory efforts can save hours to days of time spent if and when a true incident occurs. We highly recommend this as one of the most valuable and effective uses of your time spent managing cyber risk.

Business Interruption and Incident Cost Preparation

JKJ has aligned with one of the top forensic accounting firms engaged by the insurance industry, JS Held, to provide proactive consulting services to our clients to prepare them for the cost management aspect of a cyber incident. Our goal is to ensure the most coverage possible is afforded to our insured through best practice documentation procedures for costs incurred and revenue lost as a result of a cyber incident.

Ongoing Network Scans (Including Privacy Risks!)

Sick of waiting for the insurance carriers to scan your network and identify vulnerabilities that impact your coverage? JKJ has partnered with CyRisk to deliver a bi-annual network scan *in*

advance of the scans performed by the insurance carriers. Additionally, JKJ and CyRisk will perform monthly scans for the latest ransomware threat vulnerabilities and zero-day exposure detection. Participating clients will receive a report twice a year of their scan results and be notified on a monthly basis if they have a critical vulnerability associated with a known ransomware or zero-day threat. Our goal is to assist our clients in better protecting their network, and positioning ourselves to obtain the strongest terms, pricing and conditions from the insurance markets at renewal. These scans have been recently enhanced in 2023 to identify pixel tracking and other privacy related data risks that may be on your websites without your knowledge!

Anti-Social Engineering Fraud/Payment Processing Security

To this day, social engineering fraud (often perpetrated via a business email compromise) continues to be the most common cyber incident we experience with our clients. JKJ has partnered with Paymerang to deliver a solution for the growing issue of social engineering theft. Paymerang provides a streamlined invoice and payment automation platform that saves Accounts Payable (AP) departments thousands of hours annually, enhances visibility, increases accuracy, improves efficiency, and earns rebates while reducing paper, fraud risks, and operating costs.

Cybersecurity & IT Providers

Already have MFA enforced in the key areas needed to qualify for insurance? What else does your organization need to prepare to maintain strong cyber hygiene and to obtain the most competitive insurance policies? The insurance world continues to place more on more value on services with more comprehensive Endpoint Detection and Response capabilities. This includes Managed Detection and Response and Extended Detection and response (for more information on the differences, check out this great article by Crowdstrike. Additionally, there are questions about whether your organization relies upon a Security Operations Center (SOC) or has a third party to conduct a vulnerability assessment and periodic penetration testing. JKJ has a multitude of excellent resources and service providers in these areas we can avail for your consideration as you continue to enhance your cyber risk management strategy. This includes Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), and more.

Board Cyber Training

Has your Board of Directors asked you about how your organization is managing cyber risk? If they have not, then they should be! JKJ has partnered with a law firm to provide training to the Board of Directors to educate them on the landscapes of risks, their impact on the organization, and how it is and can be managed by the organization.

Contract Reviews

The devil is in the details when it comes to indemnification, liability, insurance and responsibilities assumed or transferred in a contractual agreement. JKJ will provide a non-legal review of your key contracts to provide feedback about the liability posturing of the agreement. We still advise all contracts should be reviewed by an attorney, but we can provide guidance on the language and key areas to consider. This is critically important for any key vendors or clients in your operational supply chain to ensure the proper protection of your organization's assets.

SAMPLE EXPOSURE ANALYSIS

Select Industry, Class and Annual Revenue

× Professional Services *

× Law Firms - Mixed Client Base ... *

× $300,000,000 *

Annual Revenue ($)

Estimated Records Calculator

Refine Estimated Records

Total Estimated Records*

671,866

*Based on Industry Class Median

Industry MIN

46,979

Industry MAX

4,687,312

Estimated Incident Costs

Refine Number of Records Compromised

Estimated Total Cyber Incident Costs

$9,622,764

Compromised Records: 671,866

*Incident Investigation**	$2,277,285
*Crisis Management**	$4,273,553
*PCI**	$25,000
*Fines/Penalties**	$1,017,926
Ransomware	$1,000,000
Data Restoration	$500,000
Business Interruption	$529,000

CHUBB

*In partnership with NetDiligence

Data Breach Cost Calculator

HOW MANY RECORDS WERE EXPOSED?	1000000
WHAT TYPE OF DATA WAS EXPOSED?	PII
IS THIS THE ORGANIZATION'S FIRST BREACH?	(•) Yes ( ) No
WAS THE DATA STORED IN A CENTRALIZED SYSTEM/LOCATION?	( ) Yes (•) No
IS FRAUD EXPECTED?	(•) Yes ( ) No
IS A CLASS ACTION LAWSUIT EXPECTED?	(•) Yes ( ) No
DOES YOUR ORGANIZATION CURRENTLY HAVE DATA BREACH COVERAGE?	(•) Yes ( ) No

TOTAL COST	$12,312,500
PER RECORD COST	$12

Data Breach Costs

PRINT CALCULATE

INCIDENT INVESTIGATION

FORENSICS INVESTIGATION	$1,045,000
SECURITY REMEDIATION	$1,100,000
BREACH COACH ® LEGAL GUIDANCE	$418,000
SUBTOTAL	$2,563,000

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT

CUSTOMER NOTIFICATION	$1,000,000
CALL CENTER	$75,000
CREDIT/ID MONITORING	$2,000,000
PUBLIC RELATIONS	$30,000
SUBTOTAL	$3,105,000

CLASS ACTION LAWSUIT

DEFENSE	$1,000,000
eDISCOVERY	$1,100,000
SETTLEMENT/DAMAGES	$3,100,000
SUBTOTAL	$5,200,000

PCI

FINES & PENALTIES	$0
FRAUD ASSESSMENTS	$0
CARD REISSUANCE	$0
SUBTOTAL	$0

REGULATORY FINES & PENALTIES

STATE AG	$658,500
HHS	$0
OTHER (FTC, SEC, ETC.)	$786,000
SUBTOTAL	$1,444,500

TOTAL COST	$12,312,500
PER RECORD COST	$12

Business Interruption

REVENUE INFORMATION

WHAT IS YOUR INDUSTRY TYPE? Select the industry type that most closely reflects your business operations.	Professional Services
WHAT IS YOUR ESTIMATED ANNUAL REVENUE? Enter your estimated annual revenue.	300000000
WHAT IS YOUR ESTIMATED GROSS PROFIT PERCENTAGE? This is calculated as your revenue less your directly variable costs and the resulting gross profit is described as a percentage: i.e. (revenue - variable costs) /revenue. This calculator automatically inserts the average gross profit percentage for your industry type. However, you may overwrite this percentage if you know your organization's actual gross profit percentage.	90
WHAT PERCENTAGE OF YOUR ANNUAL REVENUE IS DEPENDENT ON SYSTEMS AVAILABILITY? Estimate (roughly) how much the revenue you earn relies on your systems. For example, if you are an online retailer, your revenue depends on your systems being fully operational	50%
WHAT PERCENTAGE OF YOUR ANNUAL REVENUE OCCURS DURING PEAK SEASON? Estimate what percentage of your annual revenue is earned during your peak 6 months.	50%

EXTRA EXPENSES

WHAT IS THE ESTIMATED COST TO RESTORE BUSINESS OPERATIONS? Extra Expenses are costs that are incurred to mitigate any sales loss or to reduce the period of interruption. These expenses vary depending on the extent of the damage to the network. An example is the cost of using alternative servers. These should be discussed further with your broker when deciding on policy coverage.	500000

Business Interruption Loss Exposure

PRINT CALCULATE

Peak Season

30-DAY OUTAGE	$6,047,945
60-DAY OUTAGE	$11,595,890
90-DAY OUTAGE	$17,143,835

Off Season

30-DAY OUTAGE	$6,047,945
60-DAY OUTAGE	$11,595,890
90-DAY OUTAGE	$17,143,835

INSURABILITY REQUIREMENTS

In order to be eligible for the most comprehensive cyber insurance terms, conditions and competitive pricing, organizations today are expected to have the following cybersecurity measures in place. This list is continuing to evolve but represents a broad perspective of the insurance industry when underwriting cyber risks.

- **MULTI-FACTOR AUTHENTICATION**
  Also known as "two-factor authentication", multi-factor authentication (MFA) is used at the login process and helps to validate the authenticity that a user is who they say they are. It requires two forms of evidence that will confirm identification – most commonly seen as a password accompanied by a text with a passcode to be entered.

  Insurance carriers will be requiring businesses to have MFA enabled on email access, any and all remote access to the network, and on privileged (administrator) accounts. They will also prefer you to have MFA enabled to access your data backups. These are required by almost all insurance markets today, as having it in place would have prevented a significant number of past ransomware incidents. Many insurance markets will consider a business "uninsurable" without MFA deployed in these areas.

- **SECURED REMOTE CONNECTIVITY**
  Due to the pandemic, more people than ever before are working remotely. Along with the changes comes a lack of control, due to individuals potentially using personal devices and non-commercial grade software or unsecured remote access. Securing remote connectivity will prevent unauthorized access to an organization's information. Methods include using a virtual private network, which must also be secured by multi-factor authentication. The insurance carriers will often perform an external network scan to identify if you have any exposed ports or open remote desktop protocol, which is equivalent to leaving the door open for a hacker to enter. A good cyber hygiene practice is to periodically have a penetration test or vulnerability assessment done to identify these potential exposures.

- **SEGREGATED BACKUPS**
  Often times in a ransomware attack, the hackers encrypt not only your network, but your data backups because they are stored on the same network, leaving you no choice but to pay a ransom to restore your systems. To combat this, Insurance carriers are seeking clients to have their data backups fully segregated from the network, by storing them either offline (such as tapes) or in a separate cloud service.

Best practice again, is to have access to the backups secured by MFA! Additionally, it is imperative to periodically test the efficacy of your backups to ensure they are operating properly.

- **EMPLOYEE TRAINING & PHISHING EXERCISES**
  Employees are the gatekeepers to your organization's network. As such, they represent one of the biggest vulnerabilities. Employee training can be one of the most effective and low-cost strategies in preventing cyber-attacks. Best practice is to conduct the trainings frequently, meaning more than once a year.

  Employee training can be one of the most effective and low-cost strategies in preventing cyber-attacks as many employees, Best practices is for training to reoccur frequently. When coupled with a periodic phishing test, you can identify users who may need retraining beyond what is already required. By providing regular training and phishing exercises, employees will have the tools and the knowledge to better identify risks and fraudulent emails, and you will effectively impact the culture of your organization to take on more of a cyber security focus. Insurance carriers will be asking if you provide any such training to your user base and expect that it is being done AT LEAST annually.

- **CYBER INCIDENT RESPONSE POLICIES**
  Despite your best efforts to prevent an attack, the fact remains that you may find yourself facing a cyber incident of some sort before long. What would you do if you start to realize you in suffering a ransomware attack? This is the question you should be asking and plotting out your answer. As part of your broader Disaster Recovery and Business Continuity planning, organizations should prepare cyber-specific incident response policies. Planning in advance what steps you will take, including how you will communicate, who will be involved in decision making, and what resources you will want to engage (especially your broker and insurance carrier to engage the resources covered by your policy), can save you many hours of downtime in the event of a real attack. Furthermore, once completed, a copy of the plan should be printed out old-school style and distributed in a few places because you may not be able to access it on your company network in the event of a real incident! Insurance carriers will be asking if you have a plan, and often have resources and templates to help you in building one if you do not. And best practice is to test your plan by conducting a tabletop exercise, or simulation, of a cyber incident to see if it needs to be modified.

- **ENDPOINT DETECTION AND RESPONSE TOOLS**
  Technology is your friend, especially when it comes to mitigating cybersecurity threats. There are many available tools and platforms that will proactively monitor for threats, and alert you when they occur. Insurance carriers today expect you to have deployed next-generation antivirus software, and are even beginning to ask (and sometimes require) the deployment of Endpoint Detection and Response (EDR) solutions. EDR should be rolled out across all of the "endpoints" to your network, including servers, mobile devices, etc. It allows for continuous monitoring of these devices, but most importantly helps to isolate and prevent the spread of a threat or attack. This is something that is becoming more and more common to consider as part of your cybersecurity measures, and if you don't have it already, it should be on your radar to consider in the next year.

- **ENCRYPTION ON DATA AT REST AND IN TRANSIT**
  Data encryption protects sensitive information and mitigates the risk of a data breach. Data at rest is data that is stored in databases and therefore, not actively moving through networks. Encrypting data at rest protects an organization's data, no matter where it is stored. If an employee's device is stolen, the encryption will protect data, even after the hacker has gained access through a thumb drive. Information will look like a string of random characters when the hard drive is encrypted. This should be implemented on servers and laptops. Furthermore, data in transit is most commonly data being shared over email. There are tools available to automatically encrypt emails that contain potentially sensitive information. Insurance carriers will ask about these solutions and depending on the nature of your operations, it could be imperative that you have something in place.

- **PATCH MANAGEMENT PROGRAM**
  Updates to software are often a direct result of a bug that has created a vulnerability. The process of making these updates is called patch management, and the efficiency in addressing a vulnerability is of critical importance. Often underappreciated, having a sound patch management program is a crucial component of a sound cyber risk management program. A good (or bad) example of this is the Equifax breach of 2017 in which hackers exploited the vulnerability of a piece of software being used by Equifax that Equifax had failed to apply a critical patch for months. This attack would have been prevented if they had good internal processes around the timely deployment of patches to software.

- **VULNERABILITY ASSESSMENTS AND PENETRATION TESTING**
  Penetration testing aims to exploit weaknesses, while a vulnerability assessment can identify pre-existing flaws. Vulnerability assessments are a broad range analysis of your cybersecurity posture, both internal and external to identify opportunities for improvements. Penetration tests are exercises in which Whitehat hackers attempt to invade your network. Both should be performed by an outside party, preferably one that is separate from your existing IT service team or provider to identify any existing weakness in your network infrastructure. Best practices suggest these should be performed annually.

- **SUPPLY CHAIN RISK MANAGEMENT**
  In today's business world, we are so often dependent on the services of another organization, whether it is our insurance carriers, our cloud service providers, our supply chain vendors, or our clients. And part of these dependencies may involve the sharing of data, or access to our networks. Who you allow to access your data and systems can be the difference between enhanced security, or none at all. Keep careful track of the third-party vendors and organizations who have access to your data and examine how that access is controlled.

JKJ johnson kendall johnson

109 Pheasant Run, Newtown, PA 18940
215-579-6417 | www.jkj.com