Risk Q

CYBER RISK & PRIVACY MANAGEMENT

Cyber Insurance Limits Case Study

One of the largest property and casualty insurance companies in the nation was referred by their insurance broker to determine adequate cyber insurance limits.

risk-q.com

email
info@risk-q.com

Overview

The client is an American multi-line regional property and casualty insurance company operating in several states. The company is one of the largest property and casualty insurance companies in the nation. The client has a superior rating of A+ from the A.M. Best Company. Less than 17% of property and casualty insurance companies in the nation hold the highest distinction of "superior." The client utilizes over 1000 independent insurance agents that use their equipment and systems to conduct business.

In addition to financial stability, the company intends to remain a leader in the insurance industry through secure innovative services and products for its policyholders. To support this vision today, the CEO and executive leadership desire to implement a cyber risk management program that has the appropriate amounts of cyber insurance, identifies areas of cyber risk for proper remediation planning and measures agent cyber risk.

The client was introduced to RiskQ Inc., by Arthur J. Gallagher, the client's insurance broker to assist in determining adequate limits of cyber insurance coverage.

The Problem

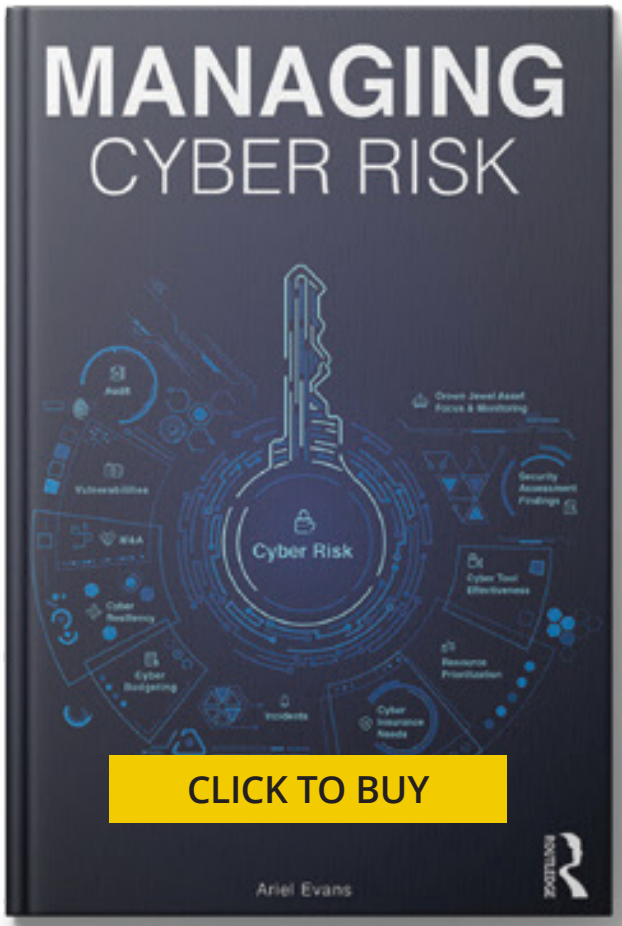
The frustration we hear in the voice of nearly every CEO, CRO or CISO is painfully acute when I am told that their cyber insurance broker cannot benchmark the amount of cyber insurance they need. Most brokers consider the use of historical purchasing data the only means to determine how much cyber insurance a company needs. Others use comparative metrics that result in a best guess at how much a company needs. I call this the Fred Rogers Method. They look for "neighboring" companies, in similar geographies, with similar numbers of employees, with similar revenues and tell them they need the same amount of insurance.

Customers are not buying it. Literally and figuratively. The issue with this approach is that it does not align to how a cyber insurance claim will be paid. Cyber is too dynamic and the use of historical data is not an indicator of how much is needed. Nor is simply having a one size fits all methodology. Cyber insurance claims are paid when there is a data breach, business interruption or for cyber extortion. The metrics to measure these are *data exfiltration exposure, business interruption exposure and regulatory exposure*. All have a relationship to the digital assets of the company. Having insurance based on these three metrics is a more effective way to limits adequacy and will give the buyer more confidence in their investment in cyber insurance.

Digital Asset Approach

In 2001, 10% of your business was a digital asset. Today, 85% of your business is in digital form. The digital asset approach is based on three years of research with the Fortune 1000 and cyber insurance industry to understand which metrics will provide limits adequacy and measure cyber resiliency. The research is the basis of the best-selling cyber risk handbook 'Managing Cyber Risk', written by the CEO of RiskQ Inc. Ariel Evans. The book is the utilized in several cyber risk courses at leading universities and outlines the use cases and metrics needed to quantify cyber exposures.

RiskQ Inc. ValuRisQ product uses the digital asset approach and a risk engine that models cyber risk in a graphical user interface. This allows each customer to model cyber risk metrics based on their needs. The interface is flexible, allows for multiple Monte-Carlo scenarios based on types of data, technologies, asset types and other digital asset parameters.



Metrics Based on Claims

Data exfiltration happens when data is stolen by cyber criminals during a data breach. This can be due to many causes including and not limited to misconfigured systems, poor access controls, from insiders or external actors. Specifically, it is the unauthorized copying, transfer or retrieval of data from a computer or server and is measured by the number of records taken multiplied by the cost per record. Data exfiltration is a malicious activity performed through various techniques, typically by cybercriminals over the Internet or other networks. On the cyber insurance policy, you may see it classified in the coverage section called “event management”. An example of data exfiltration is when an attacker sends a phishing email, a user clicks on it and malware is inserted. The attacker then delivers the payload and data is stolen to be sold on the deep and dark web for fraudulent purposes.

Business Interruption happens when business as usual is interrupted when the authorized users cannot access an application. In cyber, it is typically caused by a **denial of service attack (DoS) or a ransomware attack**. In the cyber policy you will may see this under the “network interruption” coverage section for a DoS attack. For a ransomware attack it would be under the “cyber extortion” coverage section.

Regulatory Loss happens when a regulator fines an organization for a cyber-breach. The costs of the fines are defined by the regulator(s). In the case of healthcare records, the regulatory body is the U.S. Department of Health and Human Services (HHS). For credit card data exfiltration, the guidelines are administered by the Payment Card Industry (PCI) Security Council. In the case of EU citizen data, the regulatory body is the European Supervisory Authority. There are many regulations across states for sector-based needs including the New York State Department of Financial Services Part 500, the Insurance Data Security Act, etc. Some cyber insurance policies will pay for the costs associated with the regulatory aspects of a data breach. You may see this in the cyber insurance policy as the “security and liability insurance” coverage section.

Calculating limits adequecy

Data exfiltration When determining the amount for limits associated with a cyber event, one needs to look at the worse-scenario. This is based on the highest number of records that would be breached by an attacker. The costs associated with this type of cyber incident include public relations (PR) assistance, auditing, consulting, investigation costs, communication costs, legal costs, credit monitoring, forensic costs, notification costs, call center costs and other activities that are related to ensuring the individual's whose data has been taken is being cared for and for the organization to understand why the breach happened in the first place. Cyber insurance will not pay for remediation costs. The financial exposure associated with data exfiltration is calculated by determining the highest amount of records in systems multiplied by the cost per record.

The cost per record data is available from the IBM and Ponemon Institute's "Cost of a Data Breach Report". This is an annual report of survey data of over 2,200 companies and 117 countries that shows the industry average cost per record and other breach related statistics. When we dissect these costs across the data in the report, we find that 52% of the costs per record align to what is typically insurable. 48% of costs in the report are for lost customer business, customer acquisition costs, and for free or discounted services, most of which is typically uninsurable.

Note that you will not be notifying customers twice if there are simultaneous multiple system breaches or the unique individual is in multiple systems (i.e. policy and claims systems). You are only required to notify once.

Business Interruption Financial exposures are based on the revenue lost over the period of time to get the system and processes back on-line. There are two types of limits associated with business interruption. Limits can be provided for network interruption and cyber extortion. Network interruption is the result of the denial of service attack and cyber extortion is the result of a ransomware attack. What is interrupted is the ability to transact business.

DoS attacks typically have up to a 48-hour window. The organization can restore the systems by implementing their disaster recovery plan using backups. Hopefully, the backups and the plan have been tested using table-top scenarios. A DoS attack only affects the on-premise systems of the organization. Cloud based systems are not impacted. One of the benefits of using a cloud service provider (CSP) is to have the infrastructure off-premise. Factors to determine the financial exposure related to a DoS attack are the revenue generated by each process' on-premise applications and the recovery time objective of the systems. A recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs. It is usually determined in the business continuity management processes of an organization by the system owners and the security team.

A ransomware attack happens when the attacker gains access to an organization, installs malware that restricts all users' access and a ransom is demanded to unencrypt the users' files that have been restricted. This is typically only a 24-hour event since all the organizations systems are unavailable and the organization typically opts to pay the ransom rather than restore their entire infrastructure. The 24-hour window is the time from the unavailability

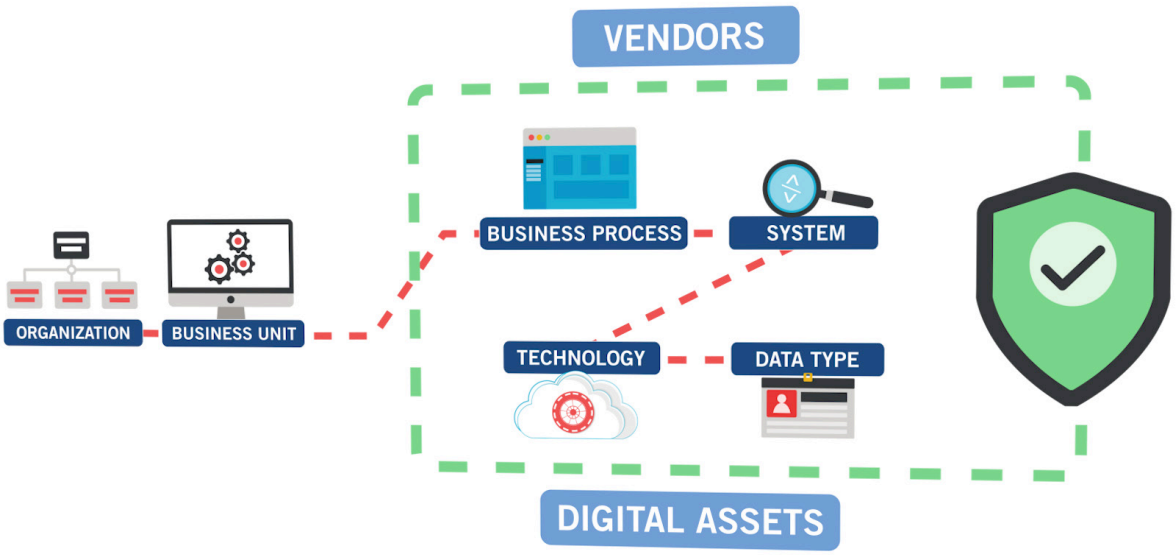
of the systems to the time the ransom is paid, and access is made available again. Activities that must take place during this time 24-hour time period include engaging internal legal counsel, outside legal counsel and forensics teams specializing in ransomware attack response who will negotiate and pay the ransom. Companies do not pay ransoms directly, they use an outside team to negotiate, pay and ensure that the attacker has not done more damage. Forensics teams will test the decryptor and ensure that there are no surprises, like a rat hiding in more malware. The factors to determine the financial exposure related to a ransomware attack are the average hourly organizational revenue, the percent of on-premise applications, the 24-hour recovery time plus the cost of the ransom itself. Ransoms typically are in the hundreds of thousands of dollars for most larger organizations, however million dollar ransoms are being seen lately

Regulatory – When determining regulatory limits, the organization has to consider a number of different factors. These include the type of data that the digital asset processes, the number of records of each data type, the level of awareness related to the breach. It is also helpful to consider recent case law when considering U.S. privacy data.

Additionally, it is critical to know the exclusions in your policy, both from a claims perspective and a cybersecurity perspective. If cybersecurity controls were reported to be in place and the forensics team uncovers that there was willful neglect, there is a strong possibility the claim could be denied.

Digital Assets Inventory

In order to start a cyber insurance quantification that provides limit adequacy the company must inventory the digital assets. **Digital assets** are systems, business processes, the data and technologies that are used as of basis of automation of work using computer technology. **Technologies** are computer related components that typically consist of hardware and software, databases, electronic communication protocols and devices. **Systems** are a consolidated set of technologies that provides the basis for collecting, creating, storing, processing, and distributing information. **Business process** is a set of digital rules that are utilized by one or more systems to take inputs, transform them and produce outputs that are reported or utilized by other systems. Data is the information that is processed and stored. When a cyber-attack occurs, the bad actor attacks the digital asset.



Digital Assets and their relationships

Doing a digital asset inventory is not a new concept. It is required when obtaining PCI, GDPR or any other cybersecurity compliance. In addition to the inventory, we also need to know the classification of the digital asset in terms of crown jewel, business critical or business crucial. **A crown jewel** impact can result in business unsustainability. **A business-critica**l attack can result in high loss but will leave the organization operational. It is important to select a cyber insurance strategy that aligns to the risk tolerance of the organization. Should you insure just the crown jewels or also business critical assets? We generally recommend ensuring against the worst-case scenario analysis and use a crown jewel strategy.

Once a digital asset inventory is complete then a record count can be done for each system to understand which systems have the most records. Each record must be unique. It is important to not double count. Most data breaches scenario analysis involves privacy records, however an organization is not limited to privacy in their analysis. Records could be credit card related, healthcare related, intellectual property or any other type of relevant classification for the company to gain insights on their levels of financial exposures. Both credit card and healthcare data are also secondarily classified as privacy data. Many companies have to comply with several regulations. In the case of a data breach, the cyber insurance costs relate to privacy data. A method to identify unique records for privacy data can be to ensure uniqueness based on the name and the social security number. The system's database administrator may advise and can run SQL queries to get the record counts for your needs.

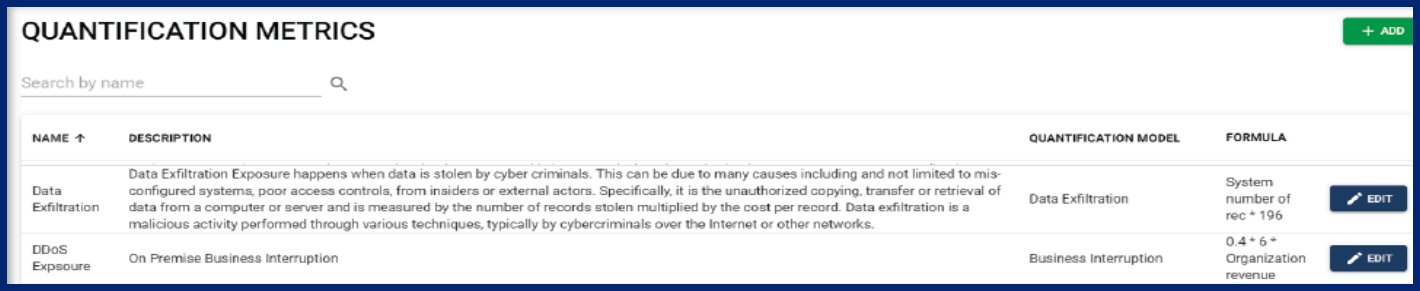
It is important to look at the record count in context. As an example, some clients did not achieve records for decades. Others when migrating to more innovative technology took all the record history. Most records older than 1-2 years serve no legitimate business purpose. Older records can be archived. Clients are advised to archive non-critical records "offline" in a database with no internet access. This will reduce data exfiltration exposure significantly. Simultaneously, it is advised to adjust the data retention policy to keep what is needed for business purposes with clear language as to how records can be achieved offline.

Companies with over 20 systems will need a product to help automate the data inventories and cyber exposure analysis. Otherwise, a spreadsheet will work to start the inventory and analysis can be done using the spreadsheet setting up macros.

How it Works

Using an Excel spreadsheet, a digital asset inventory was collected from each office that included systems (home grown and vendor supported), processes that could be interrupted in the event of a ransomware or denial of service attack, data types processed that are regulated (including privacy, healthcare, credit card, etc.) and technologies utilized (cloud services and vendor supported). A digital asset classification was used to identify which assets are crown jewels, business critical or business crucial assets. The digital asset inventory was loaded into ValuRisQ from excel and sanity checks on the information was done with the customer.

Concurrently with the digital asset inventory, risk modeling analysis was performed with the Enterprise Risk Manager (ERM) and the Chief Information Security Officer (CISO) to define the financial exposure algorithms for Data Exfiltration (data that could be stolen and result in a data breach) and Business Interruption for both Ransomware and Denial of Service Attacks. We choose a cost per record based on industry data from the IBM Ponemon Cost of a Data Breach Report. We adjusted the record cost based on what the cyber insurance policy covers to get the true cost of the record. The algorithms were modeled in the ValuRisQ risk engine.



Digital Asset Cyber Insurance Algorithms

System owners provided data for calculation of data exfiltration risk (unique record counts), providing revenue (premium income) that would be lost in the event of business interruption due to unavailability of the digital assets in ValuRisQ.

Data was analyzed in ValuRisQ to identify the appropriate amount of cyber insurance, using the algorithms for data exfiltration and business interruption. Systems with outliers were identified in ValuRisQ. An outlier is a record count from a system that has an extraordinarily large number of records. We investigated if there was a business need for those records. If there was no business, recommendations were made to archive extra records to an “off-line” system with no internet access for retrieval purposes only. Once the maximum number of unique records were identified, we had our aggregate limit based on the system with the highest record count.

Calculations in ValuRisQ were done for business interruption for DoS and ransomware attacks.

Results

The customer had a multi-million-dollar aggregate limit on their policy and lower sub-limits for cyber extortion and network interruption. They had no major regulatory exposure. The current cyber insurance limit is only about 25% of the limit needed to respond to a worst-case scenario.

The customer reported an extraordinarily high number of records in several systems. These “outliers” had record counts dramatically higher than in their other systems. The number of records reported for these systems were up to seven times higher. It appears that some records in these outlier systems have been retained for longer than needed for business purposes. It was recommended to archive the outliers down to align to the highest record count in the majority of their systems and update the data retention cybersecurity policy to reflect this need.

After the record counts from the outliers are reduced, the highest system record counts are slightly over 2 million. Other systems that are in scope have slightly less than 2 million records. It was recommended the customer increase their limits of cyber insurance by 400% based on the record cost and the maximum exfiltration of 2 million records.

DoS algorithms were set up to calculate the business interruption loss. We used the recovery time objective of 6 hours to restore crown jewel systems, the revenue processed per hour and the percentage of on-premise applications to determine the network interruption limits.

Ransomware algorithms were set up to calculate the business interruption loss. We used a time of 24 hours from demand to payment as the time frame, the revenue processed per hour and the percentage of on-premise applications to determine the cyber extortion limits.

The information was shared with the CEO and executive committee and the customer was very grateful that we were able to benchmark their needs and understand the optimal limits that they needed.

Why RiskQ

RiskQ uses an automated digital asset approach to measure financial exposures and assess cyber risk. This provides clients with objective financial data and eliminates up to 90% of the manual work by untrained personnel to perform the assessment. Clients are provided regulatory requirements/scope, policies, procedures, and automated risk assessments to be compliant with all applicable cybersecurity and privacy regulations. Our platform provides an integrated solution that is powerful, easy to use and offers the lowest total cost of ownership. In 5 simple steps you can be compliant with any cybersecurity or privacy regulation.

1. **Automated System & Vendor Inventory:** know which systems and vendors are in scope and their priority to assess. Automated Financial Exposures: understand malware, ransomware, and regulatory financial exposures.
2. Get all your policies and procedures reviewed by our **Cyber Attorneys**.
3. **Perform Security and Risk Assessments:** using any framework including ISO 27001, NIST, SOC 2, etc. Includes policies, procedures, and a playbook in layman's terms.
4. **Assess Vendor Risk:** make the vendors work for you and provide their assessment evidence in our platform.
5. **Report, Communicate and Act:** use our state-of-the-art dashboards, reports, and workflows.

About RiskQ

Based on five years of research with the Fortune 1000 and cyber insurance industry and from some of the sharpest cybersecurity and risk minds in Israel and the United States. RiskQ provides the ultimate in data loss prevention and risk management by identifying hidden exposures and making sure the attack surface is minimized and the digital assets have effective protection in place. RiskQ fundamentally alters the cybersecurity risk landscape with its digital asset approach and integrated risk platform. Get our book 'Enterprise Cybersecurity in Digital Business' free with your purchase of our offering.

RiskQ

RiskQ
66 West Flagler Street - Suite 900, Miami, FL 33130
email: info@risk-q.com
risk-q.com