WELCOME TO THE March ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

March 5, 2025

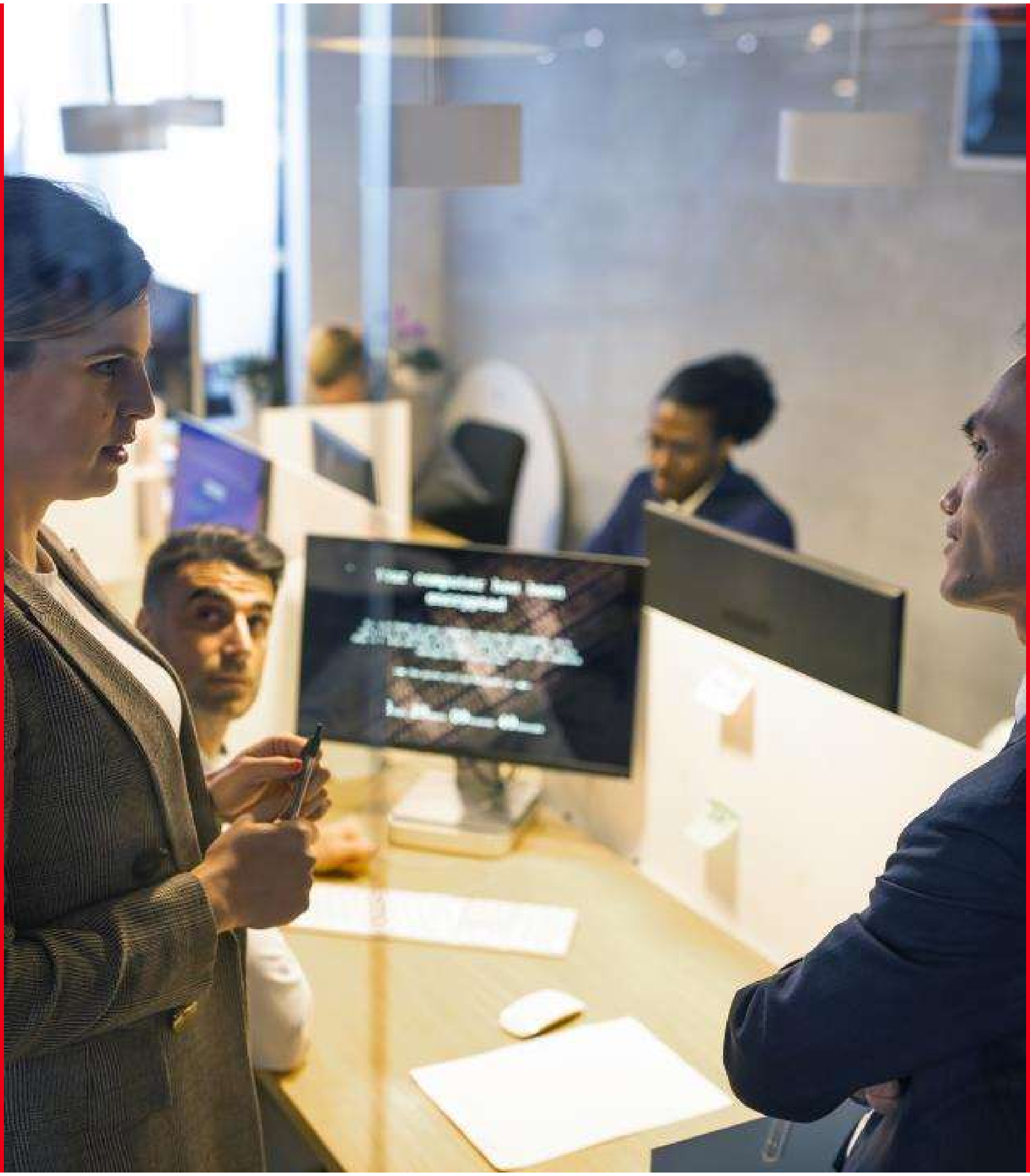
VIRGINIA IT AGENCY

Agenda	Presenter
Welcome	Kendra Burgess/VITA
Executive Branch Cyber Liability Discussion	Temo Garcia/AON
Third Party Hosted Cyber Liability Insurance	Jon Smith/VITA
TLS 1.0/1.1 Remediation	John Del Grosso/VITA
Announcements and Upcoming Events	Kendra Burgess/VITA
Adjourn	

Virginia Treasury

Executive Branch Cyber Liability Discussion

March 5, 2025



Today's Meeting

- Current Cyber Placements
  - Coverage Overview
- Cyber Market Update
  - State of the Market
  - Ransomware Update
  - Underwriting Evaluation
  - Retention / Limit / Pricing Trends
- Analytics and Risk Mitigation
- Claims Overview and Roadmap

This document has been specifically prepared for [Virginia Treasury]. Further distribution and photocopying is not permitted without the express written permission of Aon's Cyber Solutions Group. The precise coverage afforded is subject to the terms and conditions of the policies as issued. Whether or to what extent a particular loss is covered depends on the specific facts and circumstances of the loss and the terms, conditions and exclusions of the policy as issued.

Coverage Overview

1st Party Coverages

Cyber Insurance

Coverage Descriptions

Breach Event Expenses

Triggered by discovery of a privacy or security incident

Reimbursement coverage for the insured's costs to respond to a data privacy or security incident. Policy triggers may vary but typically are based upon discovery of such an event, or a statutory obligation to notify consumers of such an event. Covered expenses can include computer forensics expenses, legal expenses, costs for a public relations firm and related advertising to restore your reputation, consumer notification, and consumer credit monitoring services.

Cyber Extortion

Triggered by a threat to cause a security failure or privacy breach

Reimbursement coverage for the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat.

Digital Asset Protection

Triggered by a network security failure, unless system failure coverage provided

Reimbursement coverage for the insured for costs incurred to restore, recollect, or recreate intangible, non–physical assets (software or data) that are corrupted, destroyed or deleted due to a network security failure.

Computer Hardware Replacement

Triggered by the loss of use of computer hardware/electronic equipment

Reimbursement coverage for the insured for the replacement of computer hardware that has been rendered useless due to unauthorized reprogramming/ ransomware. Coverage is sometimes added as its own insuring agreement but is often triggered in conjunction with another insuring agreement, typically network business interruption or data restoration. As such, coverage may only apply if the computer hardware replacement would mitigate business income loss or help restore data/systems

This is a summary and is not intended to be an exhaustive analysis of all coverage items, exclusions, terms or conditions relevant to all claims and exposure situations. Please refer to the actual policy(ies) for coverage items

Cyber Insurance

Coverage Descriptions

Network Business Interruption

Triggered by a network security failure, unless system failure coverage

Business Interruption – Reimbursement coverage for the insured for actual lost net income, as well as associated extra expense, caused by a computer system outage.

- **Security Failure** – Provides coverage for interruption to an insured's business due to an interruption of an insured's computer system due to a malicious attack.
- **System Failure** – Provides coverage for interruption to an insured's business due to an interruption of an insured's computer system due to an unintentional/unplanned outage.
- **Dependent Security Failure** – Provides coverage for an interruption to an insured's business due to the outage of a computer system of a business on which the insured is dependent on caused by a malicious attack. Coverage varies but can include businesses such as information technology providers (cloud providers) or non–information technology providers. Coverage generally only extends to a dependent business where the insured has a contract in place.
- **Dependent System Failure** – Provides coverage for an interruption to an insured's business due to the outage of a computer system of a business on which the insured is dependent on caused by an unintentional/unplanned outage. Coverage varies as described in dependent security failure.

Coverage does not typically apply until after the greater of a waiting period or retention. Reimbursement periods vary greatly, but usually reimburse the insured until the restoration of computer systems (up to 120+ days).

Reputational Harm

Triggered by an Adverse Media Event during the Policy Period

Reimbursement coverage for the insured for actual lost net income as a result of an adverse media report of a network security or privacy incident. Reimbursement period (period of indemnity) varies but often ranges from 30 days to 180 days. A waiting period, usually, from 10 hours to 14 days, may also apply. Coverage may not apply if a computer system outage occurs.

This is a summary and is not intended to be an exhaustive analysis of all coverage items, exclusions, terms or conditions relevant to all claims and exposure situations. Please refer to the actual policy(ies) for coverage items

Cyber Insurance

Coverage Descriptions

Cyber–Crime

Triggered by theft of money or resources

Reimbursement coverage for the theft of money or resources. Coverage often overlaps significantly with coverage found under a commercial crime policy. Typically only offered at a small sublimit. Cyber–Crime coverage includes social engineering, invoice manipulation, computer fraud, funds transfer fraud, crypto–jacking, and telephone fraud. Coverage names/scope varies and are often intertwined.

- **Social Engineering** – Theft of money due to fraudulent instruction by a person purporting to be authorized to make such instruction (i.e. bad actor pretends to be CFO and instructs accounts payable to wire funds). May contain a condition requiring the insured to call–back or further authenticate the transaction.
- **Invoice Manipulation** – Theft of money due to the use of a computer system to manipulate payment instructions/invoices so that client/customer payments are redirected to a third party.
- **Computer Fraud–Theft** – Theft of money due to the direct or indirect control of an insured‘s computer system.
- **Funds Transfer Fraud** – Theft of money due to fraudulent instructions to a financial institution to transfer the insured‘s funds.
- **Crypto–jacking** – Theft of an insured‘s resources due to the unauthorized access to/use of an insured‘s computer systems to mine cryptocurrency that results in increased computer hosting costs and/or electricity costs to the insured.
- **Telephone Fraud** – Theft of an insured‘s resources due to the unauthorized access to/use of an insured‘s telecom systems that result in increased charges (such as toll call charges).

This is a summary and is not intended to be an exhaustive analysis of all coverage items, exclusions, terms or conditions relevant to all claims and exposure situations. Please refer to the actual policy(ies) for coverage items

3rd Party Coverages

Cyber Insurance

Coverage Descriptions

Network Security Liability

Liability coverage for defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus.

Privacy Liability

Liability coverage for defense costs and damages suffered by others for any failure to protect personally identifiable or confidential third–party corporate information, whether due to a failure of network security or not. Coverage may include: unintentional violations of the insured's privacy policy, actions of rogue employees, and alleged wrongful collection of confidential information.

Regulatory Proceedings Liability

Liability coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security. Includes coverage for fines and penalties to the extent insurable by law. Compensatory damages, i.e. amounts the insured is required by a regulator to deposit into a consumer redress fund, may be covered.

Payment Card Industry Data Security Standards (PCI–DSS)

Coverage for a monetary assessment (including a contractual fine or penalty) from a Payment Card Association (e.g., MasterCard, Visa, American Express) or bank processing payment card transactions (i.e., an "Acquiring Bank") in connection with an Insured's non–compliance with PCI Data Security Standards.

Media Liability Coverage

Liability coverage for defense costs and damages suffered by others for content–based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured's website only to all content in any medium.

This is a summary and is not intended to be an exhaustive analysis of all coverage items, exclusions, terms or conditions relevant to all claims and exposure situations. Please refer to the actual policy(ies) for coverage items

Market Update

Cyber

Cyber Liability

Q1 2025 Market Dynamics

Pricing (Consistent to Slightly Decreasing)	🟢
Capacity/Limit (Ample)	🟢
Underwriting/Process (Consistent)	🟡
Retentions (Consistent)	🟡
Coverages (Consistent)	🟡
Claims & Loss (Increased Frequency)	🟠

● Exceeds Norms
●
● Meets Norms
●
● Below Norms

Overall

Despite an increase in claims frequency in 2024 and poor loss development on 2023 claims, buyers' market conditions continued through 2024 for Cyber amidst a well-capitalized and competitive environment. On average, buyers achieved a –6.7% premium decrease in 2024. Reports of abundant and alternative (such as ILS & CAT bonds) capacity led to a favorable 1/1/25 Cyber reinsurance cycle which is a strong indicator buyer friendly markets conditions will continue into the first half 2025 for Cyber insurance purchasers.

Insureds are continuing to utilize cyber modeling to evaluate their Cyber purchasing decisions and determine the appropriate limit levels. In 2024, 21% of Aon's Cyber insurance purchasers added limits to their program.

A Look Ahead

- As we kick off 2025, insurers are closely monitoring the loss development that occurred in 2023 and the high frequency potential near systemic type loss events that occurred in 2024 (CrowdStrike, Change Healthcare, CDK, Blue Yonder, etc…). Despite those events, flat to modest rate reductions are expected to remain available as incumbent insurers are highly motivated to retain business, high excess layers on large programs have competition to drive premium down, and new capacity entrants along with high growth goals of legacy Cyber insurers in the middle market segment are driving favorable outcomes for buyers.

- Risk differentiation will remain key to insurers in 2025. To continue to showcase Insured's differentiation in the marketplace Aon has established an "Achieving Cyber Resilience Everyday" framework to guide insureds through the process of improving and demonstrating their best-in-class controls to insurers throughout the underwriting process and policy period.

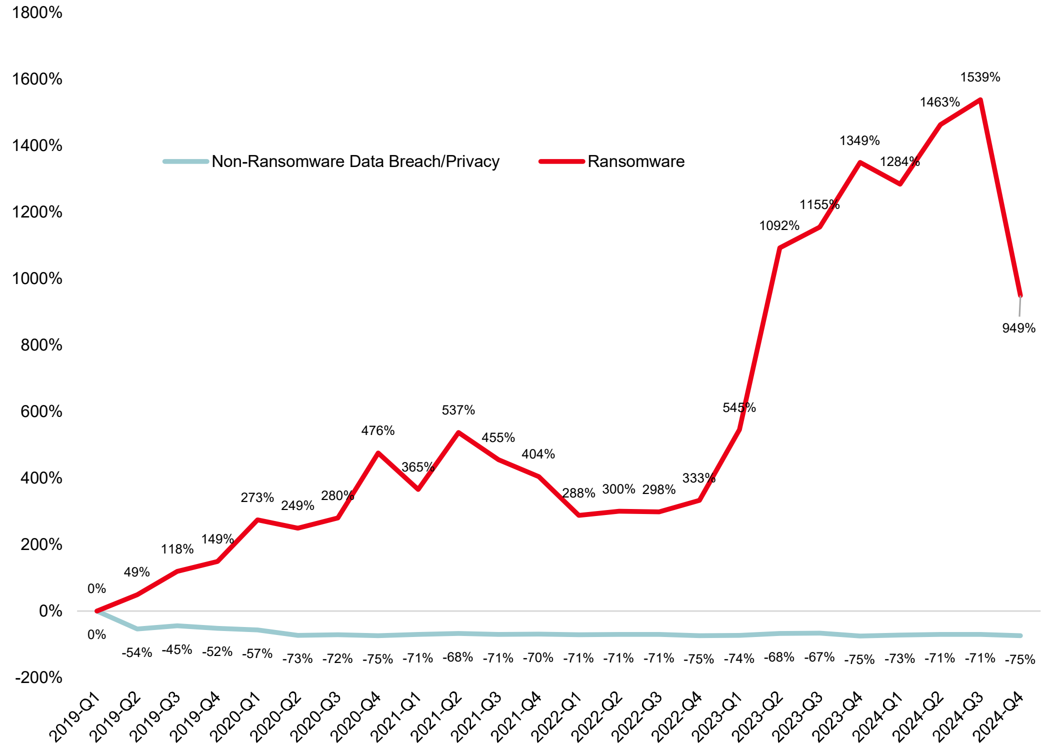
- Given the stabilizing market conditions Aon brokers are continuing to push insurers to offer differentiated and expanded coverage offerings for evolving risks/threats organizations will face in 2025 and beyond such as: expanded and streamlined business and dependent business interruption coverage, supply chain vulnerability coverage, regulatory coverage inclusive of wrongful data collection events and coverage for Artificial Intelligence creation/usage related events.

- A continuing trend into 2025 is the potential to secure a long-term agreement (LTA) or a rate guaranteed renewal to drive stability in your Cyber program. As we look forward to what may be an evolving market over the next 3-5 years due to continued decelerating rates combined with increasing claims activity, identifying the right long-term primary and excess insurer partners who understand your risk, have a proven track record of paying claims, and are willing to tailor policy wording to address your risk exposures and incident response strategies is critical.

Major Market Topics – Cyber

Artificial Intelligence	• Cybercriminals are leveraging Artificial Intelligence (AI) and machine learning to automate and scale attacks. • Insurers are interested to understand how organizations are using AI to amplify and expand their cyber security defenses. • A significant data privacy risk exists if using AI tools and platforms are being used to obtain efficiencies if they are not governed or monitored properly. • Many software development AI tools are trained on open–source code – this can be considered an unlicensed use and lead to copyright infringement claims. • Insurers are very interested in AI service offerings or the use of AI tools to enhance existing technology or professional service offerings when underwriting those risks for professional indemnity or technology errors and omissions coverage. • Adopt an AI Approach with Confidence, for CISOs and CIOs • How to Navigate AI-Driven Cyber Risks
Global IT and Supplier Outages	• 2024 saw several potential catastrophic cyber events occur. The financial impact on the global cyber insurance market is still unknown, but recent reports and the 1/1/25 cyber re-insurance cycles suggest there will be minimal impact to profitability of cyber insurers. In 2025, we do expect cyber insurers to increase the number of questions asked around the usage of supply chain vendors and cyber security platforms. • Top 10 cyber incidents during 2024 revealed | Insurance Business America • CrowdStrike Outage: Aon Cyber Solutions Update • Lessons Learned from the CrowdStrike Outage: 5 Strategies to Build Cyber Resilience
Privacy Litigation	• Insurers are continuing to review policy language and coverage related to wrongful or unlawful collection. • Privacy regulatory exposures around the world continue to become restrictive as privacy laws are added or expanded. • We are continuing to see an increase in privacy claims related to website tracking, Pixel Tracking and BIPA.
Ransomware	• Frequency of Ransomware incidents remains high and the software supply chain continues to be a target for bad actors. • Dependent Business Interruption is a significant concern for insurers as large vendor incidents can trigger numerous policies as a result of a single event. • Insurers are continuing to grapple with underwriting to systemic events that can lead to aggregation issues.

Cyber Incident Rates Indexed to Q1 2019



Source: Risk Based Security, analysis by Aon. Data as of 1/15/2025; Claim count development may cause these percentages to change over time

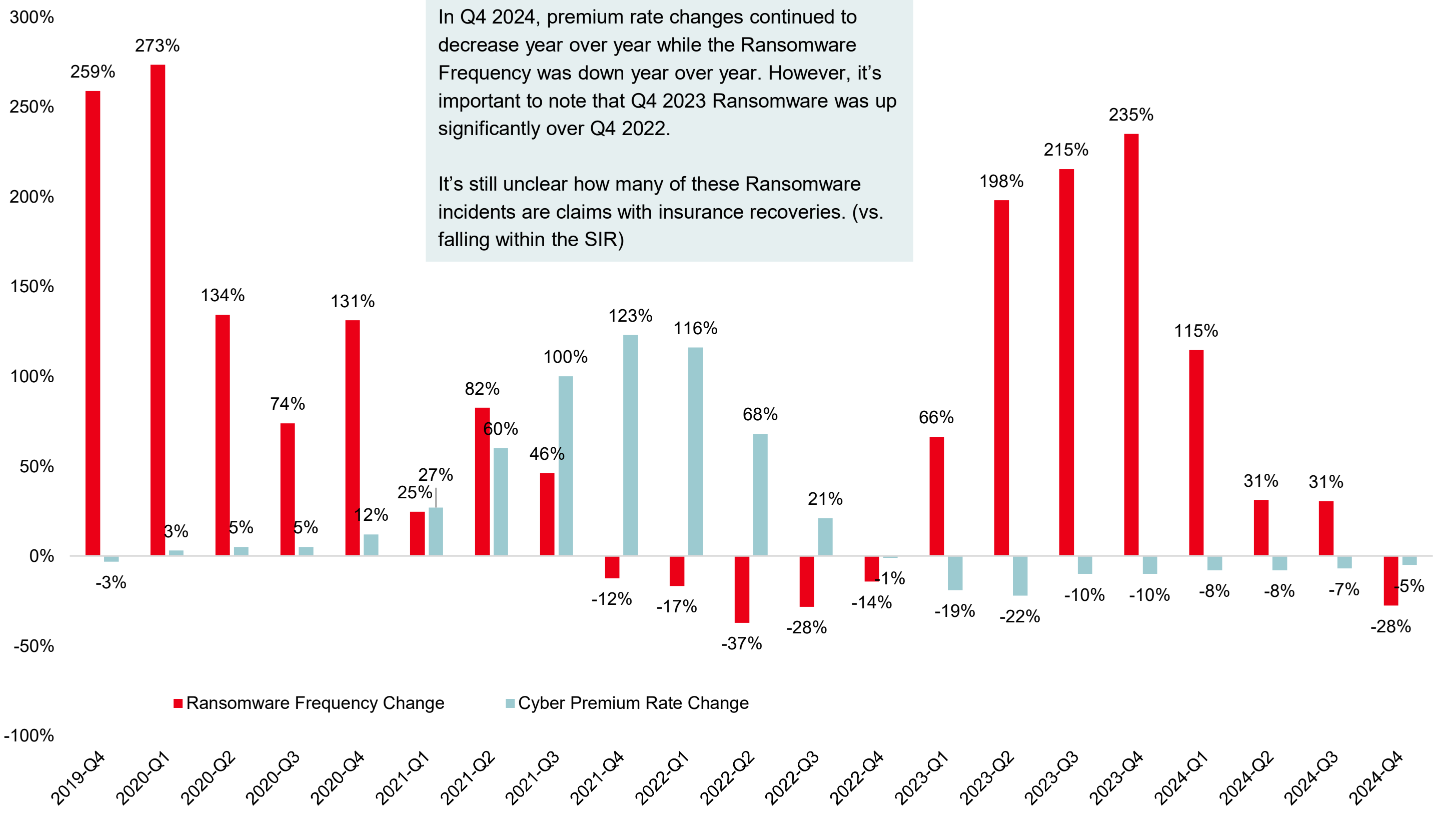
Proprietary & Confidential: The content, analysis and commentary included herein are understood to be the intellectual property of Aon. Further distribution, photocopying or any form of third–party transmission of this document in part or in whole, is not permitted without the express, written permission of Aon.

Key Observations:

- Ransomware activity was down compared to prior quarters in Q4 2024 yet continued to remain elevated compared to pre-Q1 2023
- **Ransomware Events were up 949%** from Q1 2019 to Q4 2024
- Compared to Q3 2024:
  - Ransomware Events were down by -36%; however, Q3 2024 was one of the largest ransomware quarters to date
  - Non–Ransomware Data Breach/Privacy Events were down by -13%
- The most commonly impacted industries by Ransomware in Q4 2024:
  - Business Professional Services
  - Manufacturing
  - Real Estate / Construction
  - Healthcare

Ransomware Frequency & Cyber Premium Rates

Year Over Year Change



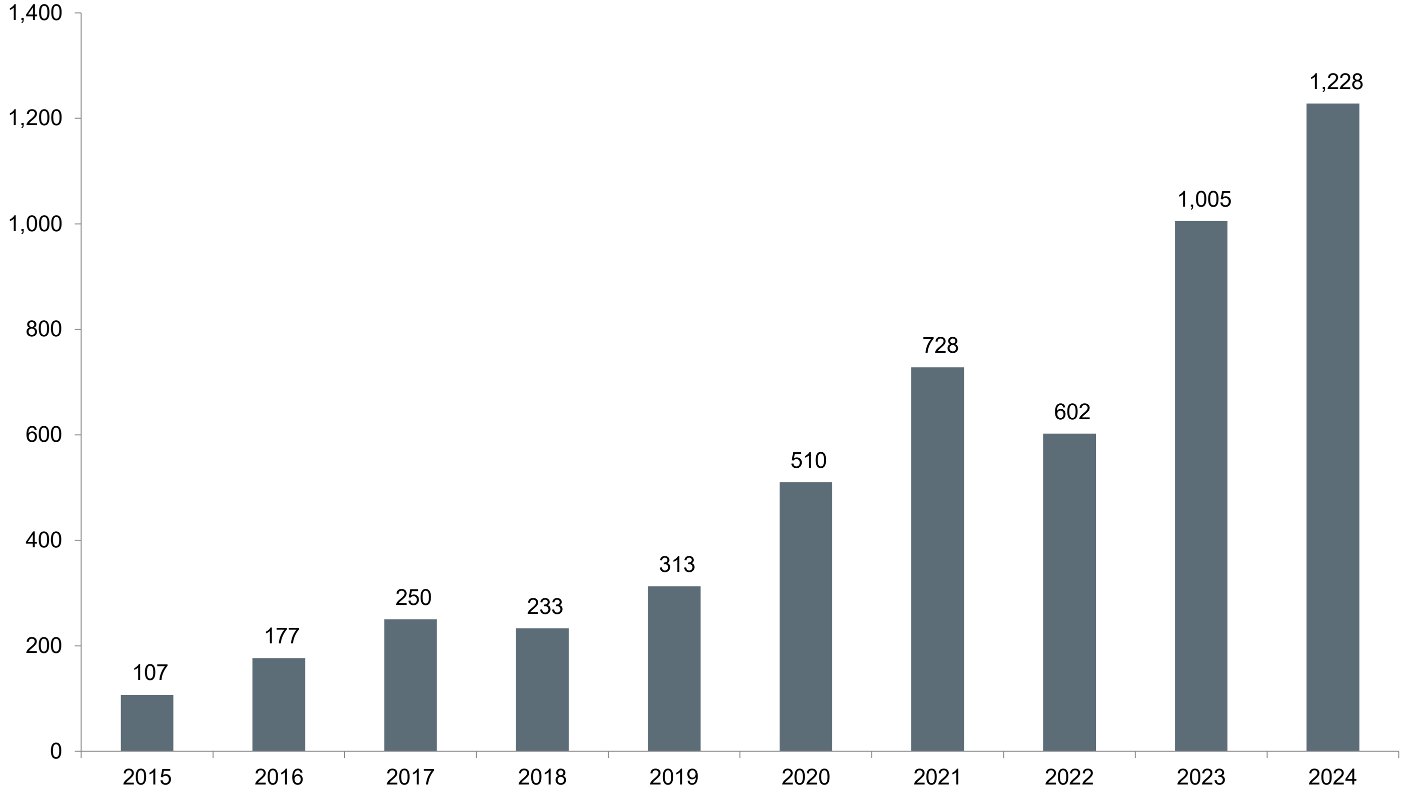
In Q4 2024, premium rate changes continued to decrease year over year while the Ransomware Frequency was down year over year. However, it’s important to note that Q4 2023 Ransomware was up significantly over Q4 2022.

It’s still unclear how many of these Ransomware incidents are claims with insurance recoveries. (vs. falling within the SIR)

Source: Risk Based Security, analysis by Aon. Data as of 1/15/2025; Claim count development may cause these percentages to change over time

Proprietary & Confidential: The content, analysis and commentary included herein are understood to be the intellectual property of Aon. Further distribution, photocopying or any form of third–party transmission of this document in part or in whole, is not permitted without the express, written permission of Aon.

Aon U.S. E&O-Cyber Broking Reported Incidents by Report Year



Source: Based on Aon U.S. E&O-Cyber Broking clients. Data through 12/31/2024.

Proprietary & Confidential: The content, analysis and commentary included herein are understood to be the intellectual property of Aon. Further distribution, photocopying or any form of third-party transmission of this document in part or in whole, is not permitted without the express, written permission of Aon.

Underwriter Cyber Concerns

What Underwriters Care About

Insurance carriers are constantly improving their underwriting processes to better evaluate insureds exposures and controls. To get the best insurance outcomes, insureds need to provide positive responses to underwriter inquiries, either through effective controls or a clear narrative, in all key areas.

Multi-Factor Authentication (MFA)	Endpoint Detection and Response (EDR)	Phishing Exercise, Cyber Awareness Training
Patch Management	Secure RDP, VPN	Incident Response Plan, Ransomware Exercice
Access Control, Service Accounts	Disaster Recovery and Backups	Email Filtering
Zero-Day Vulnerabilities and Supply Chain Risks	Network Segmentation and Monitoring	M&A DD and Integration

Underwriting Considerations

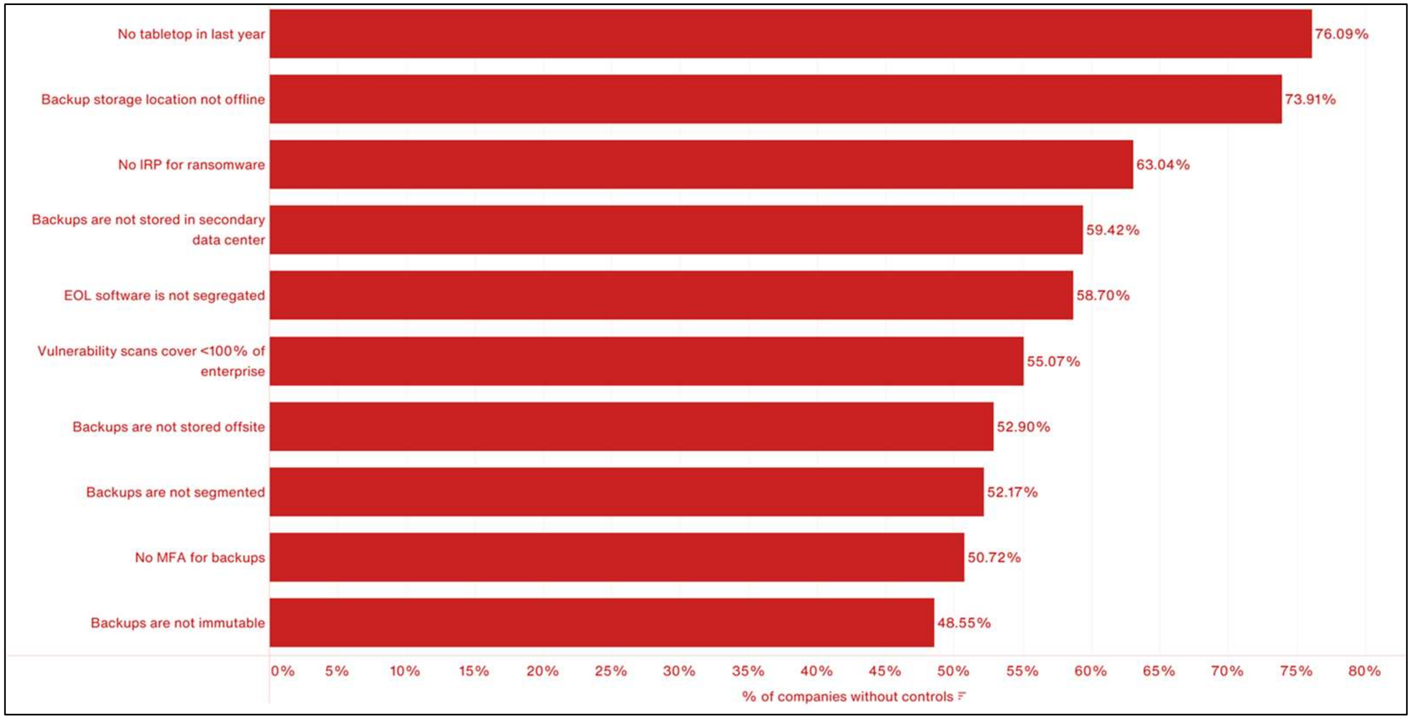
- **Budget Restrictions:** schools and local governments often have outdated technology, facilities, and funding deficiencies. Due to inadequate funding, public entities are often not able to improve cyber security.
- **Public Space Diversity:** the diversity of the public spaces create high record counts, which are common targets for ransomware attacks. Public spaces also have large networks with many EDR's that create vulnerabilities.
- **Claims Severity & Frequency Increase:** public entities are vulnerable to cyber attacks, market conditions point to increased cyber attacks with public entities being more susceptible.
- **Business Interruption Costs:** claim activity reflects a significant Business Interruption (BI) and Extra Expense exposure for public entities – this has been evidenced through high profile incidents in Atlanta, Baltimore, Pensacola, Oakland, and Greenville. Attacks disrupted operations to court systems, payment systems, police stations, sanitation services, energy departments, etc. BI plays a role in losses as the entities work to bring systems back online. Underwriters pay special attention to RTO's, disaster recovery plans and backup controls.
- **Ransomware Exposure:** ransomware continues to be the primary driver for claims. The lack of resources and up-to-date equipment make public entities strong targets for ransomware attacks. Gen AI may be playing a role in creating some phishing attacks used to deploy ransomware.
- **Privacy Exposure:** public entities have significant privacy exposure due to the nature and volume of sensitive data they process and store. Underwriters evaluate how this data is stored and what safeguards are in place to store it.

Cyber Key Controls

Marketplace Minimum Expectations

Multi-Factor Authentication (MFA)	Endpoint Detection and Response (EDR)	Phishing Exercise/ Cyber Awareness Training
Vulnerability Scanning & Patch Management	Secure RDP/VPN	Incident Response Plan/ Ransomware Exercise
Access Control/ Service Accounts	Disaster Recovery/Backups	Email Filtering & Security (DMARC / DKIM)
Zero Day Vulnerabilities and Supply Chain Risks	Network Segmentation/ Network Monitoring	M&A Due Diligence and Integration

Top 10 Red Flags for Public Entities

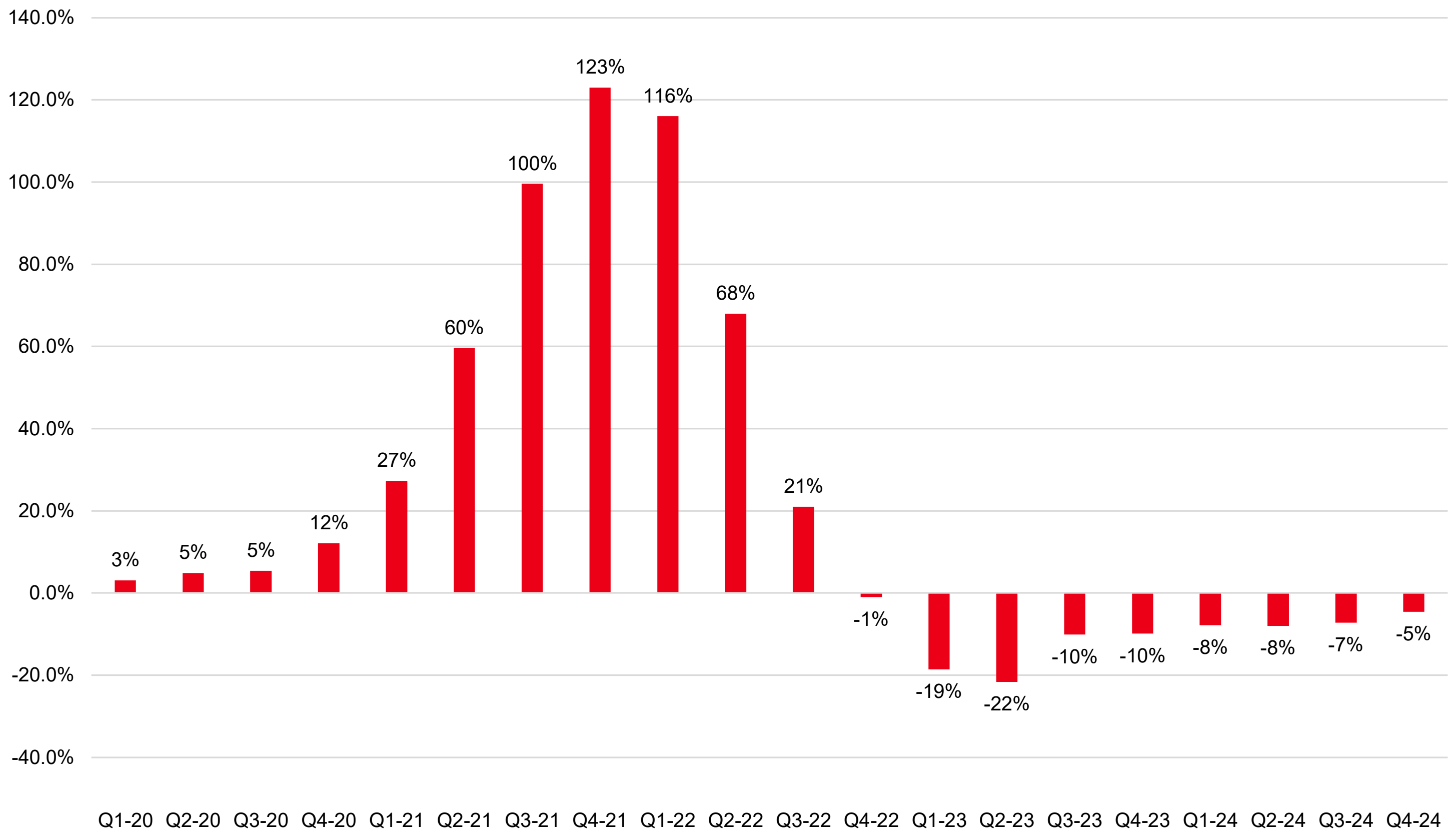


Source: CyQu Red Flags data

Proprietary & Confidential: The content, analysis and commentary included herein constitute the proprietary and intellectual property data of Aon. Further distribution, photocopying or any form of third-party transmission of this document in part or in whole, is not permitted without the express, written permission of Aon. Copyright 2024. All rights reserved.

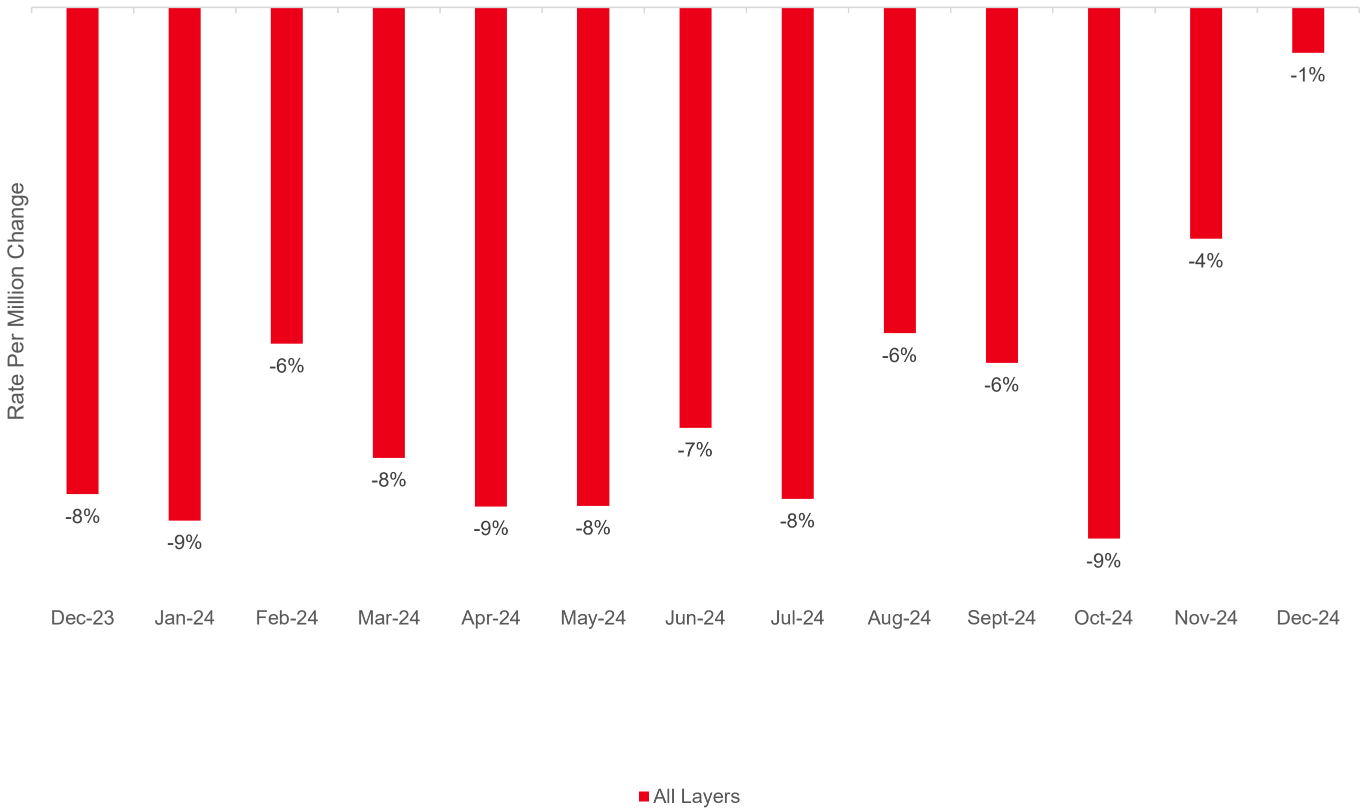
2020–2024 Cyber Premium Changes by Quarter

Average Year–over–Year Change (Same Clients)

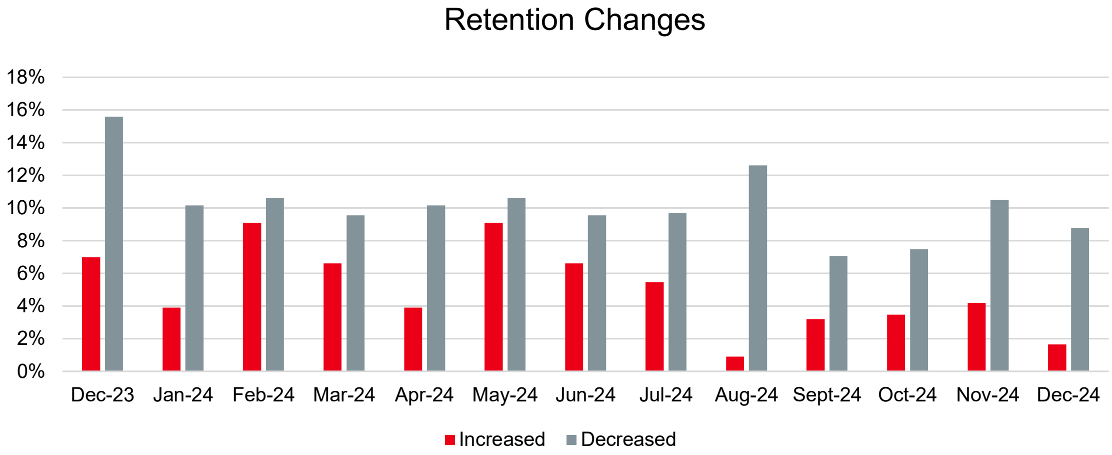


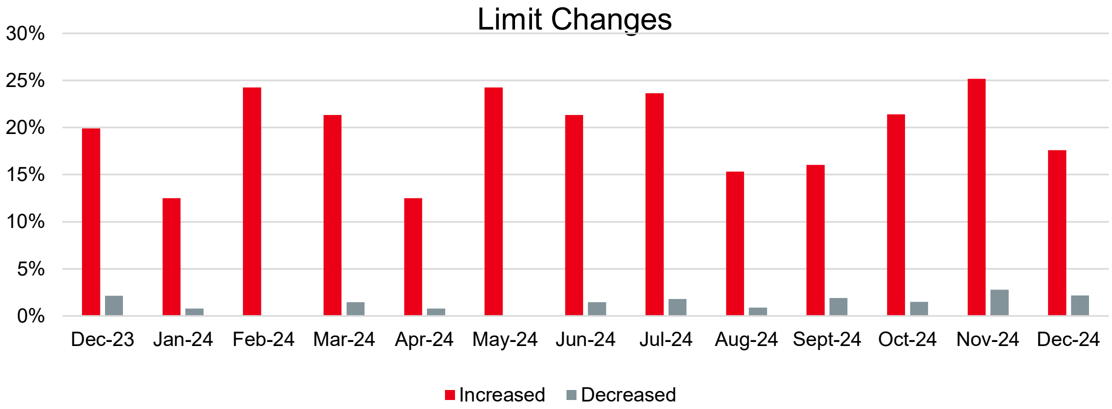
Cyber Monthly Pricing All Layers

Average Year–over–Year Change (Same Clients)



Retention and Limit Change Year Over Year





Key Observations:

- About 10% of our clients saw retention decreases in Q4. Relatively few clients experienced retention increases in Q4.
- We continued to see ~20-25% of our clients purchase additional limits in Q4, with very few choosing to decrease limit.

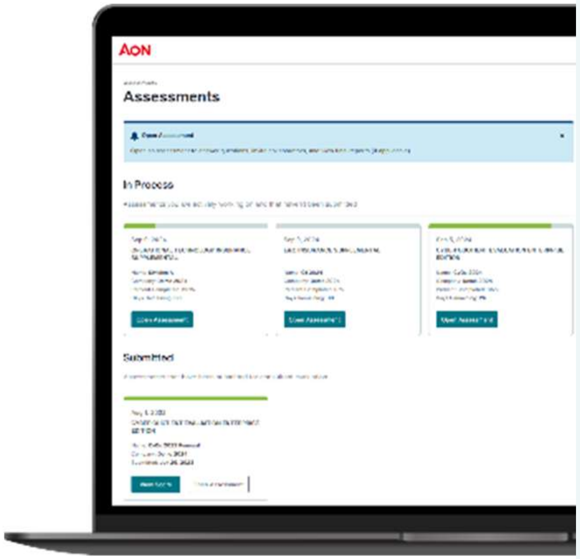
Analytics and Risk Mitigation

Better Informed Broking Process - CyQu

Enhance the broking process with CyQu

CyQu, Aon's patented[1] global cyber e-submission platform:

- Streamlines the submission process while identifying, measuring and managing a client's risk exposure
- Includes multiple insurance application question sets to support cyber, E&O and miscellaneous professional liability insurance placements
- Is accepted by the majority of Aon's largest insurance markets[2] and its insurance carrier panel



Easier Submissions and Stakeholder Collaboration

- **Assess:** Evaluate improvement opportunities and control maturity across nine critical domains.
- **Analyze and Recommend:** Flag and prioritize vulnerabilities that may impact insurability and help you triage gaps in critical controls
- **Remediate and Mature:** Prioritize security investments while optimizing risk costs. Collaborate with your account team on remediations to manage your exposure. Review with dedicated cyber broking consulting team.
- **Attract Risk Transfer:** A data-driven approach to managing security controls can help safeguard your balance sheet and better position you for insurability.
- **Enable Cyber Resilience:** Access services that will address the greater business impact of incidents. Align preparedness and prevention with response and remediation.

[1] United States Patent US 10,592,938 B2: System And Methods For Vulnerability Assessment And Provisioning Of Related Services And Products For Efficient Risk Suppression.
[2] The majority of largest cyber insurance markets, including Aon Structured Portfolio Solution for clients between $100M and $2B, accept CyQu as their main submission document. Aon Supplementals ransomware, errors and omissions, media content liability, operational technology, privacy and vendor are incorporated into and made part of any application for cyber coverage submitted by the applicant.

Better Informed

Drive Efficiencies with CyQu Portal

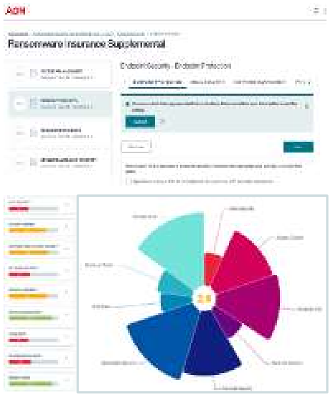
Streamline your insurance renewal, align stakeholders and utilize data insights to make better decisions and improve the submission process.

Benefits of Using CyQu Portal over Traditional “Paper” Applications

- **All-in-one interface** offers a centralized location to complete and manage the insurance application process.
- **Time-saving features**, like the ability to pre-fill submission data for the subsequent year’s renewal, even when moving between assessment versions.
- **Stakeholder alignment** by providing a framework for risk management, finance, legal, and CISO/IT team members to better work together using the “collaborate” feature.
- **Instant access to peer and industry benchmarks** to provide insights.
- **Visualize year-over year progress** and track changes in cyber maturity using the compare assessment feature.
- **Data-driven decisions** with final summary report to measure and assess risk, and an insurability analysis powered by CyQu red flags and delivered through CyQu consulting.

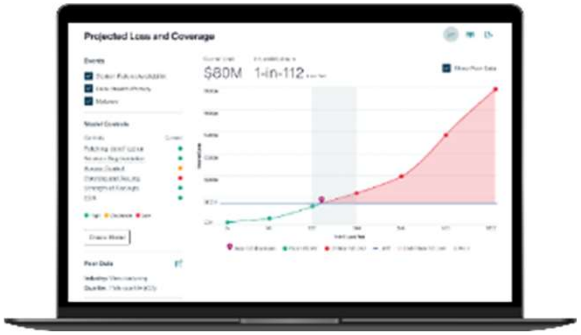
Achieving Cyber Resilience Every Day Using CyQu

Assess > Analyze and Recommend


AON
Ransomware Insurance Supplemental
Endpoint Security - Endpoint Protection

Better Informed Analytics – Cyber Risk Analyzer

Cyber Risk Analyzer helps clients take a strategic approach to cyber risk so they can help protect their balance sheets. It does more than just forecast expected loss — it **empowers risk managers** to better communicate the fundamental value that insurance provides to the C-suite, thereby promoting stakeholder alignment. .



Aon developed the Cyber Risk Analyzer to be **a powerful digital platform** which can simulate loss scenarios, contemplate security controls, and articulate total cost of risk (TCOR) **in real time**.

Cyber Risk Analyzer offers the following key features

Loss Forecasting:

Model detailed loss scenarios faster, including privacy or data breach and system failure. The tool incorporates Aon's customized proprietary simulation modelling approach based on internal claims insights, independent research by Aon's Cyber Risk Consulting team, findings from bespoke cyber modelling engagements and third-party vendor data.

Security-Controls Exposure:

Assess security-controls risks to better determine a client's loss output.

Total Cost of Risk (TCOR) Analysis:

Overlay loss forecasts with customized insurance options to produce a TCOR analysis.

Claims Overview and Reporting Roadmap

Public Entities By the Numbers

Government entities were in the top five industry classes targeted by both ransomware and business email compromise attacks in 2023, according to Artic Wolf. Additionally, the FBI reported that government entities was the third most targeted sector by ransomware in 2023.

$4.88M

2024 Avg. Total Cost of Breach, up from $.45M in 2023 (Industrywide)

$2.55M

Cost of data breach for Public Entities

$5.74M

Avg. breach costs for organizations experiencing a high-level shortage of security skills

$1M

Cost savings when law enforcement is involved in ransomware attacks

292 Days

Days to identify and contain breaches involving stolen credentials

70%

Organizations that experienced significant or very significant disruption to business operations as a result of a breach.

Top 5 Cyber Threats for Public Entities

State Sponsored Cyberattacks | Ransomware | Phishing | Hacktivists | Improper Usage & Internal Attacks

Important Notice

Claims Made Policies

Claims Made Policies

E&O/Cyber Liability policies often are claims made, which means that coverage applies to claims made during the policy period or extended reporting period (if applicable).

Reporting Requirements

E&O/Cyber Liability policies generally require reporting of claims during the policy period in which they were made. Failure to do so can result in denial of coverage.

Insurer Approval

E&O/Cyber Liability policies usually require the approval of the insurer(s) prior to selecting breach response vendors or defense counsel, incurring any defense costs, or agreeing to any settlement. Failure to do so can result in denial of coverage.

Note

The above comments are general observations. Please refer to your policy for actual terms and conditions.

This is a summary and is not intended to be an exhaustive analysis of all coverage items, exclusions, terms or conditions relevant to all claims and exposure situations. Please refer to the actual policy(ies) for coverage items

Mandatory Vendors & Resources

Beazley BBR

Forensic Services		
United States	**Canada**	**Mexico**
Stroz Friedberg, Aon Cyber Solutions	**Stroz Friedberg** Canada	KPMG
Ankura	Arctic Wolf Incident Response	Kroll
CRA – Charles River Associates	CRA	Mandiant
CrowdStrike	CrowdStrike	MaTTica
Kivu Consulting	CyberClan	Scitum
KPMG	KPMG	
Kroll	Beazley Security	
Mandiant	Mandiant	
Artic Wolf	OKiOK	
RSM	Palo Alto Networks, Unit 42	
SecureWorks		
Spear Tip		
Sylint		
Beazley Security		
Booz Allen Hamilton		

Notification and Call Center Services		
United States	**Canada**	**Mexico**
Dasher	Epiq	Business Advantage
Epiq Corporate Services	Equifax	Konecta
Experian	Miratel Solutions Inc.	Epiq Corporate Services
Intelligent Business Concepts		
Kroll		

Legal Services		
United States	**Canada**	**Mexico**
Baker Hostetler LLP	Dolden Wallace Follick	Calderon & De La Sierra
Constangy, Brooks & Prophete, LLP	Fasken Martineau DuMoulin	Davara Abogados
McDonald Hopkins LLC	Norton Rose Fulbright	Lex Informatica
Mullen Coughlin	Whitelaw Twining	R10S Abogados
Nelson Mullins		
Octillo Law		
Polsinelli PC		
Shook, Hardy & Bacon L.L.P		

Credit and Identity Monitoring
Geographically Agnostic
Equifax
Experian

Beazley panel vendor list as of January 1, 2025. For the most up to date list of providers and contact information, please click Here

Beazley Risk Management Offerings

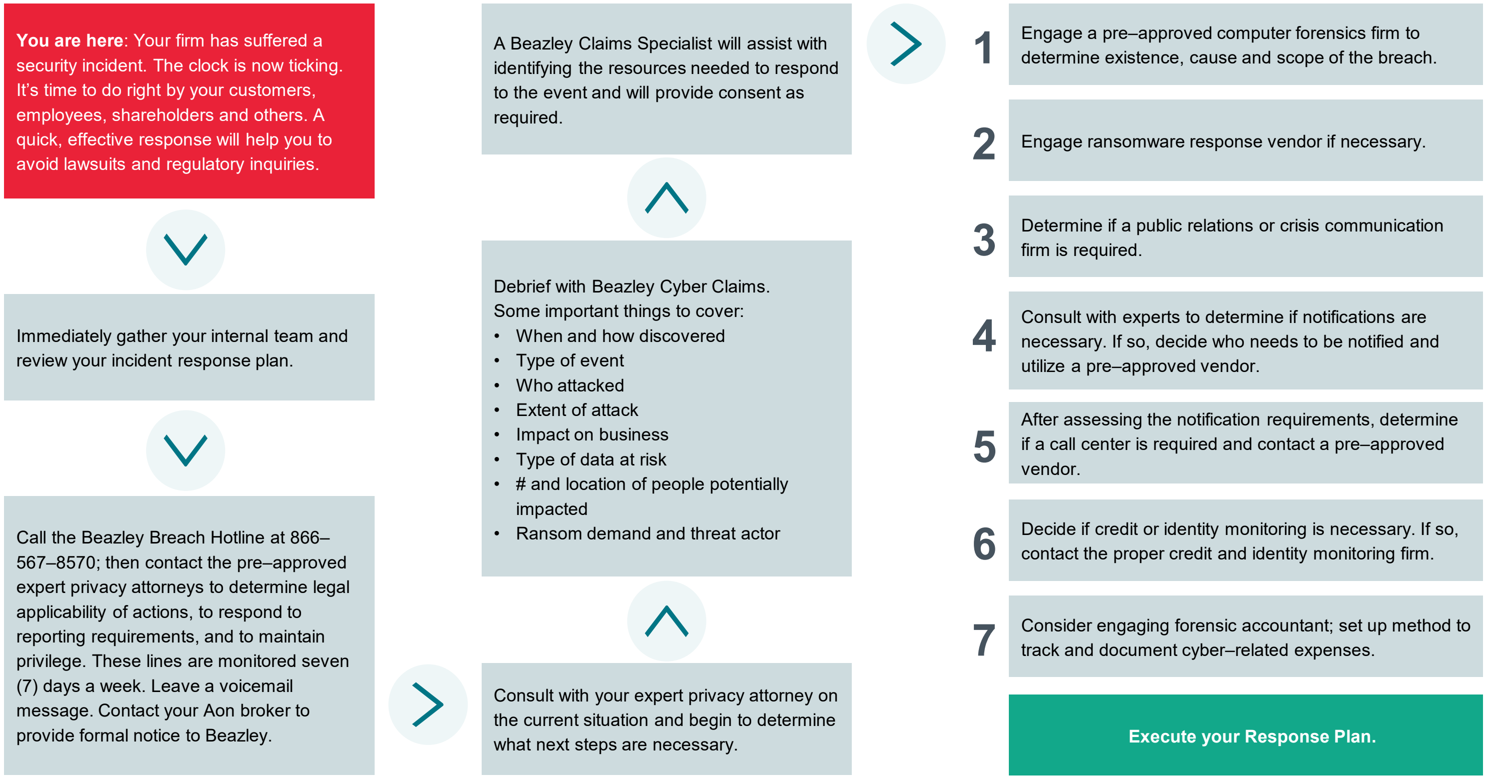
		For all cyber policyholders:	$30K+ premium:	$50K+ premium:	$100K+ premium:
Available throughout the policy period					
Risk management portal		✓	✓	✓	✓
Employee training		✓	✓	✓	✓
Vendor discounts		✓	✓	✓	✓
Risk management webinars		✓	✓	✓	✓
Onboarding video		✓	✓	✓	✓
Secure, out-of-band incident response preparation room		✓	✓	✓	✓
Onboarding call with Cyber Services*		✓	✓	✓	✓
Incident Response Plan (IRP) review*		✓	✓	✓	✓
One risk management offering per policy year					
M365 cybersecurity assessment			✓	✓	✓
Ransomware and BEC best practices workshop			✓	✓	✓
IT rationalization assessment			✓	✓	✓
Crisis communications workshop			✓	✓	✓
Crafting an IRP workshop			✓	✓	✓
Phishing-resistant MFA keys			Up to 30 keys	Up to 60 keys	Up to 100 keys
One-year phishing campaign assessment	Managed by insured		Up to 200 users	Up to 1000 users	Up to 2000 users
	Vendor-managed			Up to 500 users	Up to 1000 users
Board of directors presentation on data security				✓	✓
IR workshop with tabletop				2 hour virtual	4 hour onsite
Information security best practices session				2 hour virtual	2 hour virtual
Business continuity planning workshop				2 hour virtual	4 hour onsite
Ransomware readiness assessment					✓
C-suite/Board training on cyber resiliency					✓

*denotes clients $35M+ in annual revenue

Beazley policyholder complimentary services as of January 22, 2025. For the most up to date list of services and contact information, please click Here

Claims Reporting Roadmap

Beazley



You are here: Your firm has suffered a security incident. The clock is now ticking. It's time to do right by your customers, employees, shareholders and others. A quick, effective response will help you to avoid lawsuits and regulatory inquiries.

Immediately gather your internal team and review your incident response plan.

Call the Beazley Breach Hotline at 866–567–8570; then contact the pre–approved expert privacy attorneys to determine legal applicability of actions, to respond to reporting requirements, and to maintain privilege. These lines are monitored seven (7) days a week. Leave a voicemail message. Contact your Aon broker to provide formal notice to Beazley.

Consult with your expert privacy attorney on the current situation and begin to determine what next steps are necessary.

Debrief with Beazley Cyber Claims. Some important things to cover:

- When and how discovered
- Type of event
- Who attacked
- Extent of attack
- Impact on business
- Type of data at risk
- # and location of people potentially impacted
- Ransom demand and threat actor

A Beazley Claims Specialist will assist with identifying the resources needed to respond to the event and will provide consent as required.

1 Engage a pre–approved computer forensics firm to determine existence, cause and scope of the breach.

2 Engage ransomware response vendor if necessary.

3 Determine if a public relations or crisis communication firm is required.

4 Consult with experts to determine if notifications are necessary. If so, decide who needs to be notified and utilize a pre–approved vendor.

5 After assessing the notification requirements, determine if a call center is required and contact a pre–approved vendor.

6 Decide if credit or identity monitoring is necessary. If so, contact the proper credit and identity monitoring firm.

7 Consider engaging forensic accountant; set up method to track and document cyber–related expenses.

Execute your Response Plan.

Please note that the above flowchart is intended to serve as a high–level guide throughout the claims management process. Please refer to your policy(ies) for more affirmative guidelines regarding claims reporting and the applicability of coverage for said incident. By no means does the above flowchart represent or guarantee the applicability of coverage for each event; coverage determinations are subject to the policy terms and conditions.

Ransomware Claims

Case Studies

Case Study #1: Ransomware Payment	
Client Situation	Our client experienced a multiple-day shutdown following a severe ransomware attack. The client provided business-critical services through its public-facing website, which was subject to the shutdown. Forced to swiftly mitigate further loss, the client paid an estimated $8 million as a cyber extortion payment. Aon repeatedly engaged the cyber insurer on the client's behalf as the client negotiated and determined the need to pay the ransom.
Aon Approach	After the client made payment, the insurer was vocal in reserving the right to deny extortion coverage, on grounds such as reasonableness and adequacy of the client's attested cybersecurity measures. The insurer submitted over 30 questions in its investigation. Aon emphasized the client's demonstrated case for reasonableness and curbed the insurer's scrutiny on cybersecurity, significantly reducing the number of questions to 5. Further, Aon ensured direct engagement by the decision makers at the insurer, who had previously been primarily relying on its outside coverage counsel.
Aon Client Value & Impact	The cyber insurer timely reimbursed the ransom as well as related incident response/breach costs, a policy limit recovery of $10 million. Additionally, Aon assisted the client with its kidnap and ransom policy, which included cyber extortion coverage. Aon resolved the insurer's hesitation on the client's non-disclosure requirements and facilitated recovery of the full responsive K&R limit of $2 million.

Case Study #2: Extra Expense	
Client Situation	Our client located an advanced persistent threat on its systems. The threat was a form of ransomware, although it did not mature to point of decryption. This strain of malware is extremely sophisticated, embeds itself deep within the systems, and is difficult to eradicate. Three of the client's locations were impacted, and instances of reinfection occurred through the remediation process. To restore services and to keep malware from infecting end point devices and data, the client replaced its entire network system. The total loss was $2.8M.
Aon Approach	The insurer denied most of the loss stating this was not a ransom attack impacting data and the replacement of the system was not reasonable and necessary as this was betterment and not covered under the policy. As a threshold issue, Aon convinced the insurer that the policy did not require a ransomware event to trigger data recovery costs, as the coverage was triggered by the security event and efforts were made to restore data infected by the malware. Aon then collaborated with the client in putting together a justification for the expenses, including support that other efforts would have cost more money.
Aon Client Value & Impact	The client's position was a tough one as insurers do not fund typically fund a new system and point to reasons other than the event that support the need for the replacement. Thus, the insurer's initial response was to have a forensic review of the incident, but the client did not want to extend the dispute and potentially risk further support for the insurer's denial. Aon persuaded the insurer to negotiate based on the information provided, which ultimately led to the insurer agreeing to recognize $1.2M of the loss, much to the client's satisfaction.

Crowdstrike

Incident Summary & Impact

On July 19, 2024, Crowdstrike released a faulty update to its Falcon sensor that caused Windows computers to crash

- Falcon is a widely used EDR tool
- Microsoft estimated that 8.5 million, less than 1% of all Windows devices were impacted
- Reportedly the largest IT outage in history

Crowdstrike released a fix in under 80 minutes, but it required devices to be manually booted into Safe Mode

- By July 29, 99% of Windows sensors were back online

Full scope of incident still unknown

- Crowdstrike reported that while it has not experienced “high levels of customer churn,” it has adversely affected sales
- The error was not caused by malicious activity

Event Implications		
Financial	**Legal**	**Insurance**
• Through Q3, CrowdStrike reported that incident-related costs were over $39 million • Shares fell from $343.05 on July 18, to a low of $217.89 on Aug. 2, but have since recovered • In its Q3 financials, CrowdStrike reported that it has offered “customer commitment packages” to certain customers, which may include extended subscription periods, discounts, additional modules, professional services, and/or flexible payment terms.	• A shareholder class action and consumer class actions have been filed against Crowdstrike • Customers have sought indemnity from and/or sued Crowdstrike (Delta claims $500+ million in losses) • Crowdstrike has reported that it received inquiries from regulators concerning the outage	• CrowdStrike reports it has insurance to cover losses related to the outage, but anticipates that its coverage will not cover all costs and liabilities actually incurred • Of the Aon clients that were impacted by the July 19th outage, approximately less than 10% are pursuing coverage for losses in excess of their respective retentions

Public Entity Ransomware Cases

City, State	Demand (USD)	Recovery (USD)	Description of Event
City of Hayward, California	Not publicly disclosed	Not publicly disclosed	July 2023, the City of Hayward suffered a ransomware attack, early response did not indicate any signs of data extraction or data breach. City officials closed access to its public website and online portals
City of Oakland, California	Not Paid	Not publicly disclosed - Expected in excess of $3M	February 2023, the City of Oakland was impacted by PLAY ransomware, 610 GB of data leaked on dark web including SSN, home addresses, and medical data from thousands of current and former city employees and confidential information from residents that have filed claims against the city or applied for programs through city websites, city administrator declared state of emergency to fast-track response. Residents reported being unable to access online sites to make payments. Although calls to 911 were working, response times were delayed due to dispatching outages.
San Bernardino County, California	$1.1M	$1.9M	Early 2023, the County of San Bernardino was impacted by PLAY ransomware, over a period of one month, over $1.1M was paid to a reported Russian-linked group that infiltrated and shut down computer systems, the county paid $511,852 of the $1.1M, the remainder being paid by insurance, policy included a 50% coinsurance for ransomware related losses. Sherriff's Department was forced to shut down systems such as email, in-car computers, and some law enforcement databases, including systems used by deputies for background checks.
Clay County, Indiana	Not publicly disclosed	Not publicly disclosed	July 2024, Clay County suffered a ransomware attack that resulted in an inability to provide critical services. This attack affected all offices of the Clay County Courthouse, Community Corrections, and Clay County Probation. Local and federal law enforcement agencies were contacted. The local government declared a "local disaster emergency" that lasted for a week.
Los Angeles County, California	Not publicly disclosed	Not publicly disclosed	July 2024, The Superior Court of Los Angeles County was hit by a ransomware attack. The attack disrupted many critical systems and forced the court to shut down nearly all network systems in order to contain the damage. This resulted in 36 closed courthouses to work on recovery. The Judicial Council of California permitted the Superior Court to extend deadlines to help mitigate damages.
Washington County, Pennsylvania	Not publicly disclosed	$350,000	January 2024, Washington County experienced a ransomware attack by foreign cybercriminals. The attack seized control of the county's network and froze many of the county's operations. Hackers pilfered a large amount of sensitive information, including information about children in the court system. The county chose to pay the demand approximately two weeks after the attack.
Bernalillo County, New Mexico	Not publicly disclosed	Not publicly disclosed	In January 2022, a ransomware attack impacted the county's jail, inmates were confined to their cells due to the facility's surveillance cameras and data-collection capabilities. Court documents stated the ransomware attack led to the jail's automated doors deactivating – requiring personnel to use manual keys.
City of Chicago's Department of Aviation	Not publicly disclosed	Not publicly disclosed	An employee of the City of Chicago's Department of Aviation received an email from a provider of custodial services at Midway and O'Hare airports requesting an electronic payment of $1,150,759.82. The employee followed the instructions, it was discovered a few weeks later that the email account was compromised, and funds were recovered.

About Aon

Aon exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues provide clients in over 120 countries and sovereignties with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram. Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates. All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy. Aon does not provide legal advice. The information provided is based solely on Aon’s experience as insurance practitioners. We recommend that you consult with your own legal advisors.

About Cyber Solutions:

Cyber security services are offered by Stroz Friedberg Inc., its subsidiaries and affiliates. Stroz Friedberg is part of Aon’s Cyber Solutions which offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

Third Party Hosted Cyber Liability Insurance

Jonathan Smith

Director, Risk Management

jonathan.m.smith@vita.virginia.gov

Cyber Liability Insurance

What is cyber liability insurance?

- Insurance policy to cover organizations when they experience cyber security incidents that affect privacy, data, and network exposures and the costs associated with containment, investigation, eradication and reconstitution of application(s)/service(s) as well as costs associated with credit monitoring.
- A method to transfer risk to other organizations

What is the appropriate amount of cyber liability insurance?

- VITA has set a default amount of cyber liability insurance at $5 million per occurrence.
- Agencies should ensure that the appropriate amount of cyber liability insurance is required of the supplier.

Cyber Liability Insurance

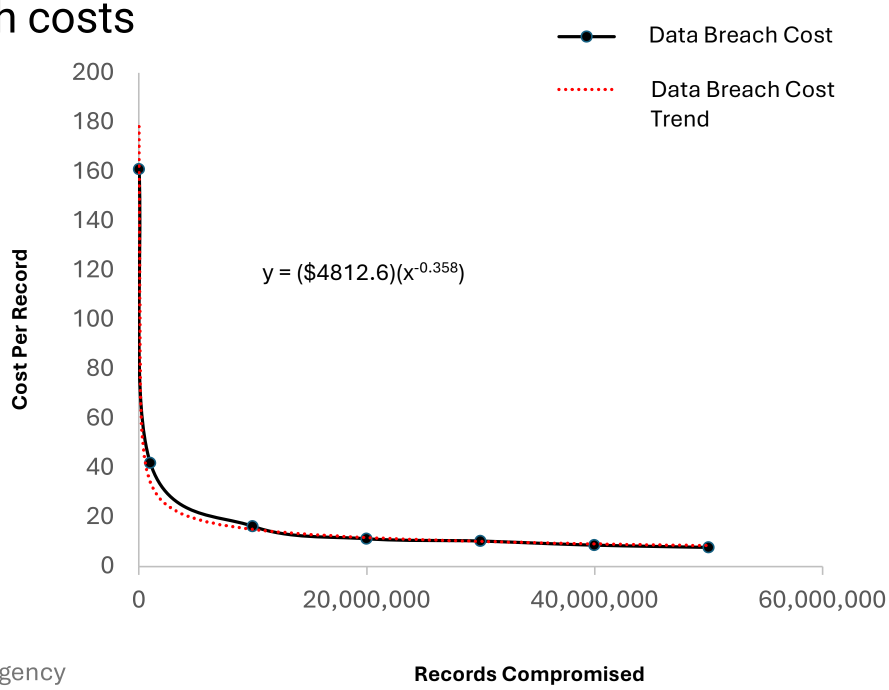
What do we need to estimate the amount of cyber liability insurance?

- A description of the application/service and the business processes that it will support.
- Will the application/service process and/or store sensitive data with relation to confidentiality, integrity, and/or availability?
  - If yes, please describe the sensitive data (i.e. confidentiality - PII, PHI , integrity - financial records , availability - public safety data).
- Approximately how many records will the application/service process and store?
- Approximately how many (max) unique individuals may be impacted in the event of a cyber security event?

Cyber Liability Insurance

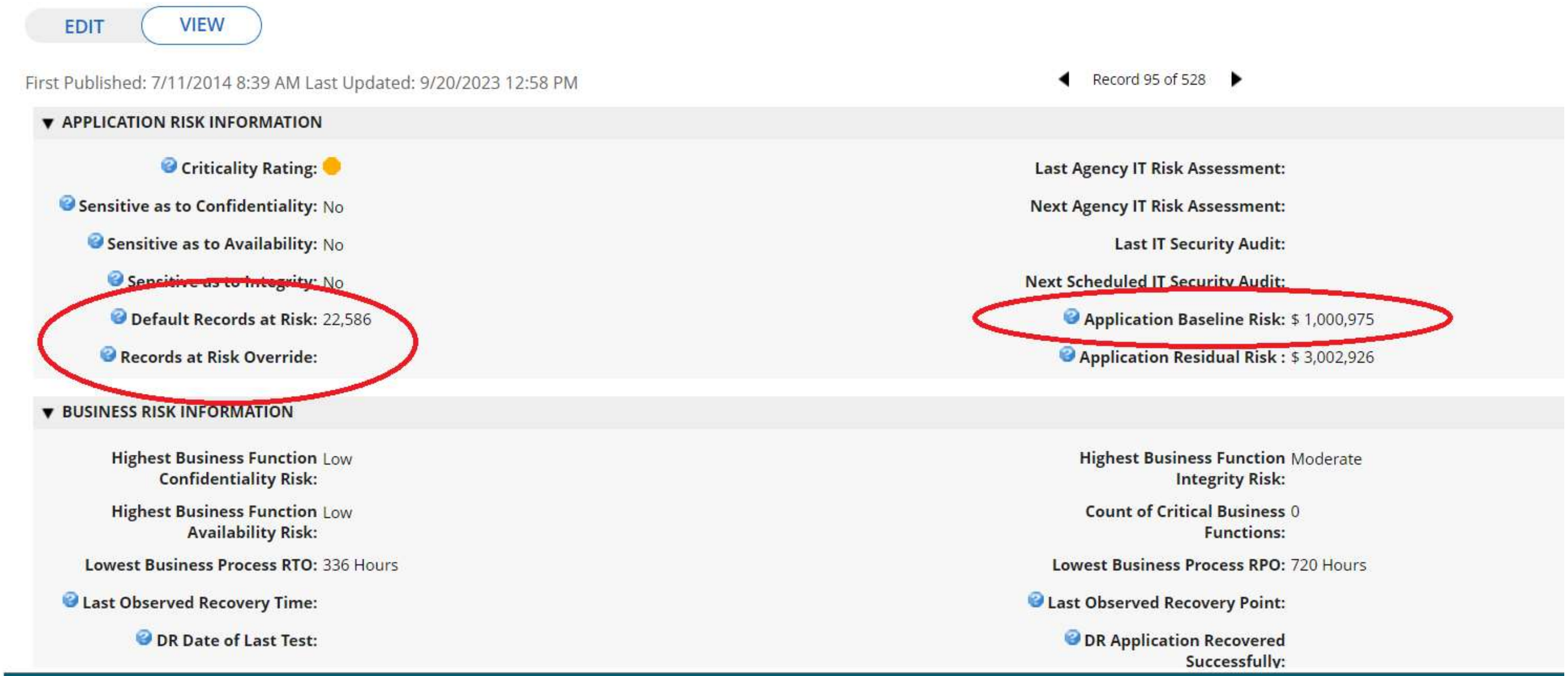
Cyber liability insurance calculation

- CSRM developed a methodology to estimate costs associated with the detection, response, and recovery activities associated with cyber security incidents.
- Based on industry trends and Commonwealth costs
- Formula based on a decaying 'line of best fit'



Cyber Liability Insurance

Cyber liability insurance calculation – Archer eGRC



First Published: 7/11/2014 8:39 AM Last Updated: 9/20/2023 12:58 PM

Record 95 of 528

▼ APPLICATION RISK INFORMATION

Criticality Rating:	●	Last Agency IT Risk Assessment:	
Sensitive as to Confidentiality:	No	Next Agency IT Risk Assessment:	
Sensitive as to Availability:	No	Last IT Security Audit:	
Sensitive as to Integrity:	No	Next Scheduled IT Security Audit:	
Default Records at Risk:	22,586	Application Baseline Risk:	$ 1,000,975
Records at Risk Override:		Application Residual Risk :	$ 3,002,926

▼ BUSINESS RISK INFORMATION

Highest Business Function Confidentiality Risk:	Low	Highest Business Function Integrity Risk:	Moderate
Highest Business Function Availability Risk:	Low	Count of Critical Business Functions:	0
Lowest Business Process RTO:	336 Hours	Lowest Business Process RPO:	720 Hours
Last Observed Recovery Time:		Last Observed Recovery Point:	
DR Date of Last Test:		DR Application Recovered Successfully:	

Questions?

Jonathan Smith

Director, Risk Management

jonathan.m.smith@vita.virginia.gov

VIRGINIA IT AGENCY

TLS 1.0/1.1 Remediation

Enterprise Project

John Del Grosso, SSDC Service Owner

Encryption protocols have gone end-of-life

Release	Release date	End of life
TLS 1.3	March 2018	
TLS 1.2	August 2008	
TLS 1.1	April 2006	June 30, 2018
TLS 1.0	January 1999	June 30, 2018

- Transport layer security (TLS) 1.0 and TLS1.1 are end-of-life
- There were several extensions due to COVID and other industry-related delays
- All TLSv1.0 and v1.1 must migrate to TLSv1.2 or TLSv1.3

Deprecation of TLSv1.0/v1.1

Nearly every agency has some in-motion data that is using either TLSv1.0 and/or v1.1 within the data centers in the COV and going outside the COV.

Process to identify sources:

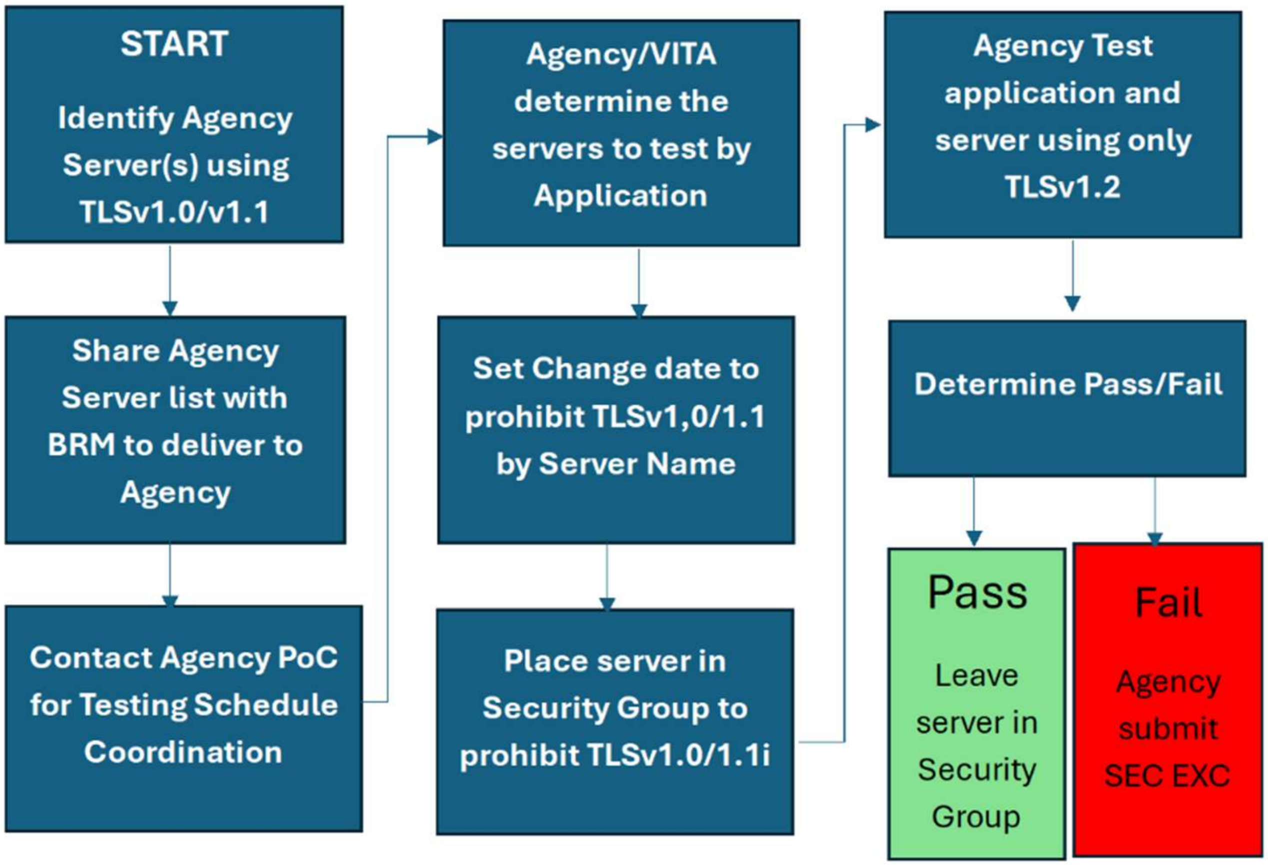
The Unisys and multi-sourcing service integrator (MSI) teams have used Atos 'Tenable' data and other sources to identify the servers, ports and TLS versions that have been detected as using v1.0 and v1.1.

Next steps:

The next step is for the team to determine the best and least intrusive method to limit all server ports to only using TLSv1.2. Those will incorporate direct means (specific to a server) or global means. The team will work directly with each agency for complete collaboration.

To ensure operations are not negatively impacted, no changes will be made globally.

Process diagram



START

Identify Agency Server(s) using TLSv1.0/v1.1

Share Agency Server list with BRM to deliver to Agency

Contact Agency PoC for Testing Schedule Coordination

Agency/VITA determine the servers to test by Application

Set Change date to prohibit TLSv1,0/1.1 by Server Name

Place server in Security Group to prohibit TLSv1.0/1.1i

Agency Test application and server using only TLSv1.2

Determine Pass/Fail

Pass

Leave server in Security Group

Fail

Agency submit SEC EXC

How agencies can help get ahead of the end-of-life deprecation

1. Determine if your agency-owned application(s) support use of v1.2
2. Check the operating system (OS) settings. If the OS security settings on a server have been changed to allow ‘any’ TLSv1.x, to change those switches back to TLSv1.2+ only
3. If agency applications cannot support TLS1.2+, then submit a security exception(s) in Archer to identify the server name and agency application, along with the remediation actions required.

Questions?

Announcements

ISOAG March 5, 2025

Nucleus User Guides Are Here!

Hey ISOs! The Nucleus User Guides are now live on the CSRM Connections website!

Learn how to:
✅ Access & analyze vulnerabilities
✅ Prioritize risks effectively
✅ Streamline workflows & boost security

View the guides today on CSRM Connections
(Under the "ISO Resources" link on the right side)

Strengthen your agency's security with ease! 🔐

SPLUNK UPDATE – 🌈Strike Gold with Your Splunk Logs! 🍀

Just like finding a pot of gold at the end of the rainbow, now is the perfect time to identify the logs you want ingested into the VITA Splunk instance!

VITA is partnering with agencies to bring your application logs into Splunk, helping you uncover valuable insights and strengthen security.

Don't let your logs stay hidden like leprechaun treasure—let us know which logs you need ingested.

We're always happy to schedule a call to discuss your options and ensure everything is ready to go.

Let's make sure your logs shine like a lucky four-leaf clover this year! 🍀

Top 5 Vulnerabilities

For the Month of March, the Top 5 Key Vulnerabilities are:

- **KB5044343 Windows Server 2012 R2 Security Update (October 2024)**
- **KB5043138: Windows Server 2012 R2 Security Update (September 2024)**
- **Oracle Java SE Multiple Vulnerabilities (October 2018 CPU) (Unix)**
- **Microsoft .NET Core SEoL**
- **IBM Java 6.0 < 6.0.16.75 / 6.1 < 6.1.8.75 / 7.0 < 7.0.10.35 / 7.1 < 7.1.4.35 / 8.0 < 8.0.5.25 Multiple Vulnerabilities**

FYSA

Staff Changes

- Chris Williams is the Director of Enterprise and Security Architecture.

Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

Service Tower SOC Report Review Sessions

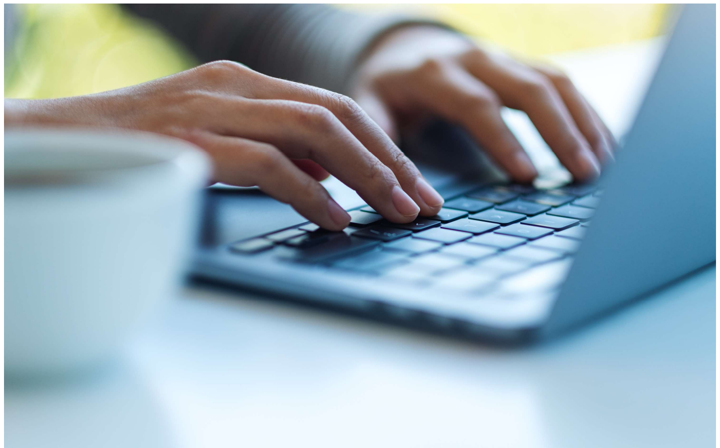
The upcoming SOC review session is March 11, 2025, and will be held remotely.

Please register at the link below

To register for this meeting, please click on the link below:
https://covaconf.webex.com/weblink/register/re1ad0ac90a496f42b7a8bcb25d01f763

IS Orientation

The next IS Orientation is being held in March



- March 26, 2025, from 9am to 4pm, registration closes March 19th.
- It will be held **in-person** at the Boulders location:

  7325 Beaufont Springs Drive, Richmond, VA 23225

- Visit Commonwealth IS Orientation to register!

https://forms.office.com/Pages/ResponsePage.aspx?id=qeUKYsFOoE-GQV2fOGxzCdWeH7DmIQxlu_AIelbJ-HRUMjdNWUs0RVlCSUVCSUxMRzYxMk84MU5LNi4u

PUBLIC SECTOR NETWORK

Government Cybersecurity Showcase Virginia
Elevating Virginia’s Digital Defense

Public Sector Network is presenting: Government Cybersecurity Showcase Virginia

Held on Wednesday, April 9, 2025, at the **Downtown Richmond Marriott**

- The registration link is below:

[Public Sector Network » Event - Government Cybersecurity Showcase Virginia]

Commonwealth of Virginia Information Security Conference 2025

Future-Proofing Cybersecurity:

Next-Gen Strategies

August 14, 2025

Hilton Richmond Hotel, 12042 West

Broad St., Richmond, VA 23233

Registration will open soon!

MEETING ADJOURNED

VIRGINIA IT AGENCY