

LISA LEWIS, DIRECTOR
STEPHANIE BONNETT, ASSISTANT FINANCE OFFICER
FREDA HOLDERMAN, ACCOUNTING SUPERVISOR

DEPARTMENT OF FINANCE

TO: Board Members
FROM: Lisa Lewis, Director of Finance *llw*
DATE: July 10, 2024
RE: Cyber Policy

Please see the attached quote for cyber insurance. I ask the Board to approve renewal for the cyber insurance plans with Assured Partners through Corvus Insurance.

OUR MISSION IS TO INSPIRE AND EQUIP OUR STUDENTS TO SUCCEED IN LIFE

BULLITT COUNTY PUBLIC SCHOOLS IS AN EQUAL EDUCATION AND EMPLOYMENT INSTITUTION



 CORVUS Quote

Smart Cyber Insurance

for Bullitt County Board of Education

Produced June 04, 2024

Producer

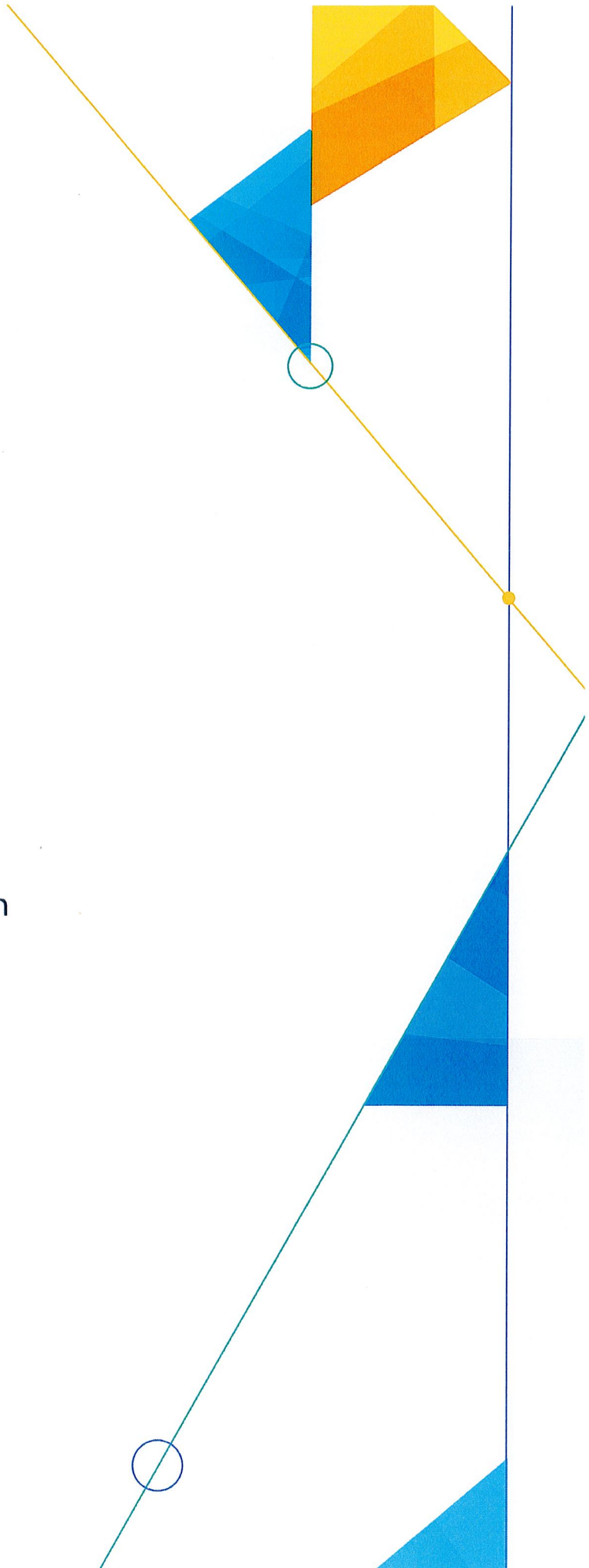
Dillon Behr, RPS Insurance
dillon_behr@rpsins.com

Underwriter

Peter Hedberg

Corvus Insurance

100 Summer Street, Suite 1175, Boston, MA 02110
www.corvusinsurance.com



Bullitt County Board of Education scores 82 out of 100 overall

And ranks in the 59th percentile relative to industry standards. This calculation is based on other companies with similar industry class and annual revenue.

Learn more about this report: <https://help.corvusinsurance.com/the-corvus-scan-how-it-works-and-what-to-expect>



Scanned: Jun 04, 2024

Breakdown of Corvus Scan Findings

In addition to calculating an overall Corvus Score and benchmark percentile, the Corvus Scan organizes specific issues identified by the Scan into categories based on the impact to overall cyber risk: **Critical**, **High**, **Medium**, and **Low**. Together, these findings cover several key dimensions of an applicant's security posture. The full Corvus Scan Report provides specific recommendations for any Actionable Findings to reduce risk exposure to your business.



Preview of Recommendations

BACKUP & RECOVERY

RANSOMWARE ASSESSMENT

Implement a robust backup solution.


Critical

Finding

The vCISO assessment determined that your organization's backup solution may be missing a key redundancy.

RANSOMWARE ASSESSMENT

ENDPOINT SECURITY

Leverage an Endpoint Detection and Response (EDR) solution.

■
Critical

Finding

The vCISO assessment discovered that your organization does not currently use an Endpoint Detection and Response (EDR) solution or Next Generation Anti-virus (NGAV) solution.

Beyond the DLP: Cyber Risk Resources

Policyholders enjoy access to an online dashboard featuring Corvus's virtual Chief Information Security Officer (vCISO) Center. Within the vCISO Center, policyholders can view their latest scan findings and find a prioritized list of actions to improve their cyber security posture. They'll also find a vendor marketplace with vetted, industry-leading cybersecurity solutions offering discounts for Corvus policyholders.

See our Services Guide to learn more: [Learn More Here](#)

[Bind with Corvus for additional recommendations and the full DLP Report](#)

You are at **lower risk** of a ransomware attack based on our cyber risk model.

1 Risky Open Ports Detected

A high number of open ports across a network is an indicator of a larger attack surface. We focus on remote administration ports as they are targeted at a higher rate.

No Software Vulnerabilities Detected

Our risk model considers critical and high vulnerabilities from the national vulnerability database for relevant software detected on your public infrastructure.



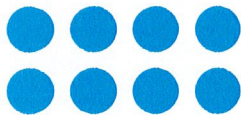
Ransomware
Risk Score

Ransomware by the Numbers

Regardless of how sophisticated your business' IT security infrastructure is, ransomware is always a threat.

8 in 10

include the threat to leak stolen data



More than 8 in 10 ransomware attacks (through Q2 2021) involved the threat to release exfiltrated data to increase leverage ([Coveware](#))

31%

of cyber claims



For all businesses with up to \$2bn in annual revenue, ransomware accounts for nearly 1/3 of cyber claims, making it by far the leading cause of loss. ([Net Diligence](#))

\$142,637

average payment



Average ransomware payment in 2021 (through Q3) among Corvus policyholders.

Best Practices To Reduce Your Risk



Improve resiliency

Maintain & test backup strategy; ensure software is kept up to date; train employees to recognize phishing; use multi-factor authentication for critical systems.



Know your risk

Assess your IT environment for vulnerabilities by reviewing the full DLP report delivered upon binding your policy, and test your employees to identify phishing risk.



Monitor your environment

Watch for suspicious behaviors on your network or devices, ensure security technologies are deployed & actively monitored, and check vulnerability alerts from Corvus.

Partner with Corvus

Not sure where to start? Learn More: [Learn More Here](#)

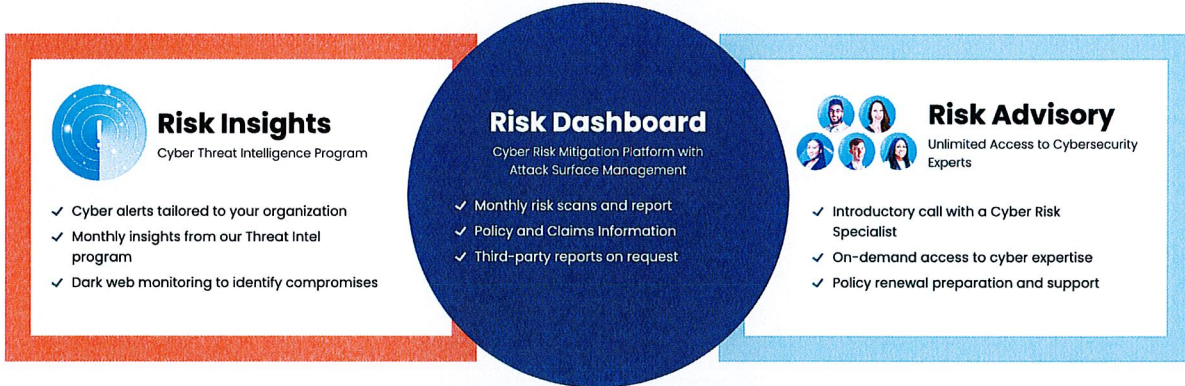
Our Risk and Response Services, available for all policyholders, include hands-on help in reviewing and prioritizing cybersecurity practices.

Corvus Signal™

The risk prevention solution for Corvus policyholders

Stay ahead of emerging cyber threats and optimize security spending with the solution shown to reduce the frequency of cost of breaches by nearly 20%. The solution is available at no cost with any Corvus policy (estimated value: \$86,000 per year).

Your personalized Corvus Signal™ services include:



Risk Insights

Cyber Threat Intelligence Program

- ✓ Cyber alerts tailored to your organization
- ✓ Monthly insights from our Threat Intel program
- ✓ Dark web monitoring to identify compromises

Risk Dashboard

Cyber Risk Mitigation Platform with Attack Surface Management

- ✓ Monthly risk scans and report
- ✓ Policy and Claims Information
- ✓ Third-party reports on request

Risk Advisory

Unlimited Access to Cybersecurity Experts

- ✓ Introductory call with a Cyber Risk Specialist
- ✓ On-demand access to cyber expertise
- ✓ Policy renewal preparation and support

Plus: Reduce your policy retention with the Corvus Signal™ endorsement

In addition to helping reduce risk, engaging with Corvus Signal can reduce claim costs. Following a few easy steps will ensure your organization is eligible to reduce your claim retention by up to 25%. See details in your quote below.

Corvus Signal™ benefits by numbers

20%
lower

frequency and cost of cyber breaches

\$86k

estimated value in services available at no cost to Corvus policyholders

15.5
days

average head start before alerted vulnerabilities are exploited by threat actors

3x

faster patching, with cyber alerts sent the same day as discovery

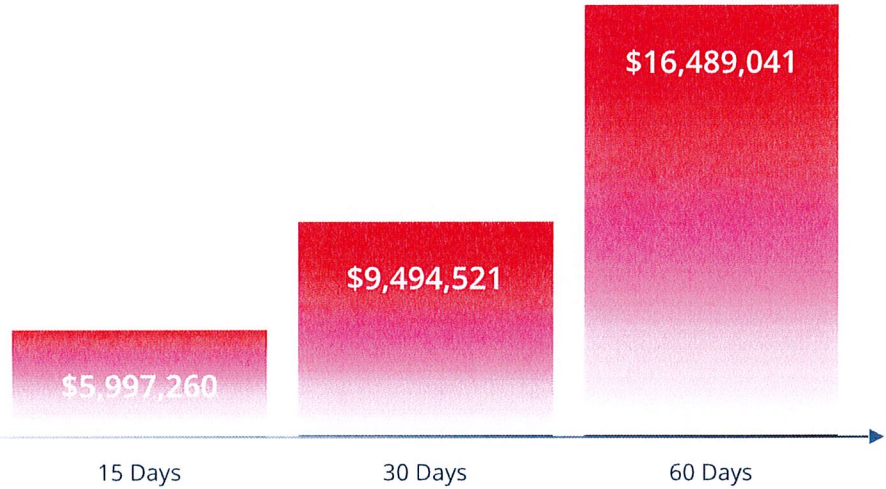
See our website page for more information:

<https://www.corvusinsurance.com/corvus-signal>

Estimated Business Interruption Cost

Total cyber loss estimates may be greater, as this calculation does not include:

- regulatory fines and penalties
- PCI-DSS assessment expenses
- cyber crime/financial fraud
- reputational loss



Approximating the Ransomware Risk

In a ransomware event leading to a shutdown of all operations, what might the approximate cost be?

Your Annual Revenue		\$115,000,000
Cost of Goods Sold	-	26%
Net Annual Business Interruption Expenses	=	\$85,100,000
Percentage of Revenue Reliant on Operational Computer Systems	×	100%
Divided over 365 Days	÷	365
Daily Business Interruption Cost		\$233,151
Ransom Payment	+	\$1,000,000
Data Recovery Costs & Extra Expenses	+	\$500,000
Breach Response Costs	+	\$1,000,000

This calculation is an approximation of the cost of a ransomware event that shuts down the operations of an organization. If the organization does not rely on digital assets and tools for all of its operations then this recommendation may be too high and the recommendations should be discounted accordingly.

Cost of Goods Sold percentages are based on sources including eRiskHub and NYU/Stern (Jan. 2020) and other Corvus data; COGS estimates are recommendations only and should be adjusted for individual company costs.

Corvus recommends that each company consult further with their accountants and insurance broker in order to produce a more exact time-based recommendation.

The non-Business Interruption numbers are estimates, based on the client's revenue, and may include digital forensics, customer notification, public relations, and other first party breach response expenses.

SMART CYBER INSURANCE™ QUOTE

June 04, 2024

Named Insured	Bullitt County Board of Education State: Kentucky
Producer of Record	RPS Insurance 525 W Van Buren St Ste 1325 Chicago, IL 60607 Through Corvus Insurance Agency, LLC
Policy Period	From 07/01/2024 to 07/01/2025 Both dates at 12:01 a.m. Standard Time at the address of the named Insured as stated herein.
Retroactive Date	None; Full Unknown Prior Acts
Insurer	Travelers Excess and Surplus Lines Company (Non-Admitted, AM Best "A++" Superior)
Breach Response Hotline	Corvus Smart Cyber Insurance® 24/7 Breach Response Hotline: (855) 248-2150

Third Party Insuring Agreements	Limit	Retention
<input checked="" type="checkbox"/> A. Network Security and Privacy Liability	\$1,000,000 Each Claim / Aggregate	\$25,000 Each Claim

Claims against you because of a network security or privacy breach. This may arise from a denial of service attack, malicious code, a stolen laptop, or any type of data breach.

<input checked="" type="checkbox"/> B. Regulatory Investigations, Fines and Penalties	\$1,000,000 Each Claim / Aggregate	\$25,000 Each Claim
---	---------------------------------------	---------------------

Defense and civil fines and penalties imposed by a governmental agency as a result of a breach of privacy regulations.

<input checked="" type="checkbox"/> C. Media Liability	\$1,000,000 Each Claim / Aggregate	\$25,000 Each Claim
--	---------------------------------------	---------------------

Claims against you arising from the release or display of your media material. This includes claims alleging copyright infringement, slander, libel, defamation, and other media perils.

<input checked="" type="checkbox"/> D. PCI DSS Assessment Expenses	\$1,000,000 Each Claim / Aggregate	\$25,000 Each Claim
--	---------------------------------------	---------------------

Forensic investigation costs, fines, penalties and assessments you are legally responsible for as a result of actual or alleged non-compliance with Payment Card Industry Data Security Standards.

<input checked="" type="checkbox"/> E. Breach Management Expenses	\$1,000,000 Each Claim / Aggregate	\$25,000 Each Claim
---	---------------------------------------	---------------------

Breach response costs for which you have contractually indemnified a third party for a security or privacy breach.

First Party Insuring Agreements	Limit	Retention, Waiting Period, & Period of Indemnity
<input checked="" type="checkbox"/> A. Business Interruption See Video: www.corvusinsurance.com/bi	\$1,000,000 Each Loss / Aggregate	Waiting Period: 8 Hours Period of Indemnity: 6 Months
Business income loss and extra expenses you incur during a computer network outage.		
<input checked="" type="checkbox"/> B. Contingent Business Interruption See Video: www.corvusinsurance.com/bi	\$1,000,000 Each Loss / Aggregate	Waiting Period: 8 Hours Period of Indemnity: 6 Months
Business income loss and extra expenses you incur during a network outage at your outsourced service provider.		
<input checked="" type="checkbox"/> C. Digital Asset Destruction, Data Retrieval and System Restoration	\$1,000,000 Each Loss / Aggregate	\$25,000 Each Loss
Digital asset loss and related expenses you incur as a result of a security breach, privacy breach, or administrative error.		
<input checked="" type="checkbox"/> D. System Failure Coverage	\$1,000,000 Each Loss / Aggregate	Waiting Period: 8 Hours Period of Indemnity: 6 Months
Business income loss, extra expenses, and digital asset loss you incur during an unintentional or unplanned outage.		
<input checked="" type="checkbox"/> E. Social Engineering & Cyber Crime Coverage See Video: www.corvusinsurance.com/1st-party	\$250,000 Each Loss / Aggregate	\$25,000 Each Loss
Financial fraud, phishing attack loss, and telecommunications fraud loss you sustain as a result of a social engineering event or impersonation attempt.		
<input checked="" type="checkbox"/> F. Reputational Loss Coverage	\$1,000,000 Each Loss / Aggregate	Waiting Period: 2 Weeks Period of Indemnity: 6 Months
Business income loss you may suffer related to a media report arising from a privacy breach, cyber extortion threat, or phishing attack.		
<input checked="" type="checkbox"/> G. Cyber Extortion and Ransomware Coverage See Video: www.corvusinsurance.com/1st-party	\$1,000,000 Each Loss / Aggregate	\$25,000 Each Loss
Your expenses or payments to respond to a cyber extortion demand or ransomware attack.		

First Party Insuring Agreements	Limit	Retention, Waiting Period, & Period of Indemnity
<input checked="" type="checkbox"/> H. Breach Response and Remediation Expenses See Video: www.corvusinsurance.com/1st-party	\$1,000,000 Each Loss / Aggregate	\$25,000 Each Loss

Your expenses to respond to a data breach incident including legal services, forensics investigation, notification, credit monitoring and public relations.

<input checked="" type="checkbox"/> I. Court Attendance Costs	\$250,000 Each Loss / Aggregate	\$25,000 Each Loss
---	------------------------------------	--------------------

Expenses you incur to attend court, adjudication, mediation or other hearing in connection with a covered claim.

Maximum Policy Aggregate Limit: \$1,000,000

Endorsements	Limit
CB-308-001 Amend Specific Legislation Endorsement	
CB-107-002 Bodily Injury Claims	\$250,000
CB-126-002 Bricking	\$1,000,000
CB-194-001 California Consumer Privacy Act	
CB-288-001 Corvus Signal Endorsement	
CB-202-001 Coverage for Certified Acts of Terrorism	
CB-123-001 Criminal Reward Expenses	\$50,000
CB-136-001 Forensic Accounting Coverage	\$50,000
CB-111-003 GDPR Coverage	
CB-133-001 Invoice Manipulation Loss	\$250,000
CB-128-001 Loss of Funds Exclusion Carveback	
CB-153-001 Pay on Behalf	
CB-148-003 RPS Cyber Amendatory	
CB-274-003 Smart Cyber Insurance Amendatory Endorsement	
CB-120-001 Solicitation Claims	\$50,000
CB-159-001 Utility Fraud Coverage	\$250,000
CB-167-001 War Exclusion Cyber Terrorism Carveback	

Premium, Taxes & Fees

Premium	\$25,047
TRIA	\$250
Policy Fee (Fully Earned)	\$195
Total*	\$25,492.00

Surplus line tax and stamping fee calculations are provided for informational purposes only. These have been provided at the request of the surplus broker. Corvus does not warrant such calculations are compliant with state law. It is the sole responsibility of the surplus lines broker to accurately calculate and file the surplus line taxes and stamping fees.

* Some taxes not applied. Contact your agent for more details.

POLICY FORM

Corvus Smart Cyber Policy Form #CB-101-001

SUBJECTIVITIES

The proposed quoted terms are valid for 45 days and subject to the receipt, review, and acceptance of the following information and are based on the representation that there are no open or unreported claims, unless previously addressed herein, as of the date of this quote. The applicant must also pass a sanctions list check which Corvus will perform prior to binding. If at any time before binding we are made aware that a claim was reported, we reserve the right to rescind or revise the terms of this quote. If an insured elects to bind coverage during this period, the effective date of the policy must be within 45 days of the date on which the quote was issued.

Due prior to binding coverage:

- TRIA Waiver if coverage is rejected (attached to quote).
- Confirmation that the Applicant does not collect, capture, purchase, receive through trade, or otherwise obtain biometric identifiers or biometric information (including, but not limited to, iris scans, fingerprints, fingerprint, voiceprint, or scan of hand or face geometry).
- Please note the limit and/or retention requested do not fit our current auto-quoting eligibility. We have offered the closest available option(s). Please contact your underwriter with any questions.
- Confirmation that the Applicant requires out-of-band authentication prior to executing an electronic payment. (Out of band authentication is a secondary verification method with the requestor of a funds transfer through a communication channel separate from the original request.) More information can be found here - <https://help.corvusinsurance.com/securing-funds-transfers-out-of-band-authentication-and-other-considerations>
- A completed, signed and dated Corvus Smart Cyber Application. Please note we will need favorable responses to bind including: Segmented backups updated at least weekly; Email filtering; MFA for email access; MFA for remote access; Access Management Solution for privileged accounts; EDR or NGAV with 3rd party monitoring.

Due within 7 days of binding coverage:

- A completed Surplus Lines Certificate.
- Please provide policyholder contact information (client name, policyholder name, email, job title) to grant access to the Corvus policyholder resource dashboard upon bind.

TAXES & FEES

This insurance has been placed with an insurer not licensed to transact business in the Commonwealth of Kentucky but eligible as a surplus lines insurer. The insurer is not a member of the Kentucky Insurance Guaranty Association. Should the insurer become insolvent, the protection and benefits of the Kentucky Insurance Guaranty Association are not available.

If the risk is subject to surplus lines tax, you must arrange for the filing of the affidavit and for payment of applicable state tax and fees, in addition to the premium.

Policy Issuance Fee: \$195

CORVUS BLACK PREMIER RISK MITIGATION SERVICES

Bullitt County Board of Education Qualifies for Corvus Black

Because this account has over \$100m in annual revenue, your client qualifies for additional free risk management services to better predict, prevent and prepare for cyber incidents.

Some of our Premium Risk Management Services Include:

- ✓ Scan Your Insured's Vendors
- ✓ "Welcome to the Flock" Onboarding Call
- ✓ Virtual Incident Response Tabletop Exercise

Learn More: www.corvusinsurance.com/corvus-black