CORVUS

Guide to Common Subjectivities and Solutions

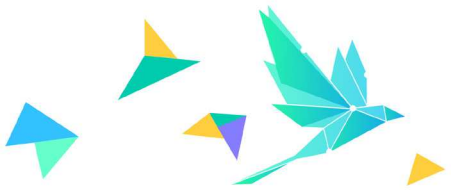
Subjectivities may be added to your Corvus Smart Cyber or Smart Tech E&O insurance quote. These are steps that the underwriter has required be completed before the policy can be bound or issued. Each of the common subjectivities discussed below have been demonstrated to significantly reduce cyber risk; in addition to helping you to obtain insurance, they will make your organization less likely to experience an incident.

The goal of this guide is to help you work through these common subjectivities and understand what resources Corvus has available to help you to meet the specifications.

Table of Contents

CORVUS

Multi-Factor Authentication (MFA)



What is MFA?

Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification methods in order to gain access to an account. Rather than just asking for a username and password, MFA requires additional verification factors, which decreases the likelihood of a successful cyberattack. Typically MFA involves a combination of *something you know* (a password or PIN), *something you have* (a code or token generated by a cell phone app or other hardware), and/or *something you are* (a fingerprint or face scan).

Where are policyholders required to implement MFA?

MFA is required for:

- **Email Access:** On-premise email servers or cloud hosted email servers.
- **Remote Access:** Anything that allows access into your internal environment or access to SaaS-based applications that store PII, PHI, or any other critical information.
- **Administrator Access:** Accounts that give full access to a system like local administrator accounts and domain administrator accounts (privileged user account access).
- Internal usage of **privileged accounts**, such as local administrators or domain administrators, should also be secured with MFA where possible — or be protected by compensating controls such as the use of a privileged account management (PAM) solution that stores privileged account credentials and unique local administrators' credentials, and can rotate them after use.
- For services accounts where MFA will not be applicable, we recommend using other cybersecurity best practices, such as a Privileged Account Management (PAM) solution to manage those, and all, privileged accounts.

Put simply, companies should look to **secure any remote access points to their systems or data with MFA.**

Why are policyholders required to implement MFA?

MFA helps protect against a large number of unauthorized access events, including data breaches and password-based cyberattacks. Fortunately, MFA is an affordable option to further protect your organization. Notably, through Microsoft 365 and Google Workspace, MFA is available for free at all license levels, making them great solutions for smaller organizations. For larger organizatinations, enterprise solutions such as DUO or Okta typically integrate with most systems already in use and provide additional security and monitoring features.

CORVUS

Multi-Factor Authentication (MFA)

What resources are available to help policyholders implement MFA?

For email and cloud, major cloud email providers like Microsoft 365 and Google Gmail or Workspace have a free MFA solution, regardless of the subscription level purchased. Many cloud software comes with free MFA solutions that just need to be turned on, especially software that is used to store sensitive data (such as Electronic Medical Records software and HR software).

- Official Microsoft documentation
- GSuite Documentation

For remote access, policyholders should check whether the VPN or other remote access tool that they use has MFA as a free option. If not, they will need to identify an MFA tool that integrates with their software or hardware, such as Duo or Okta.

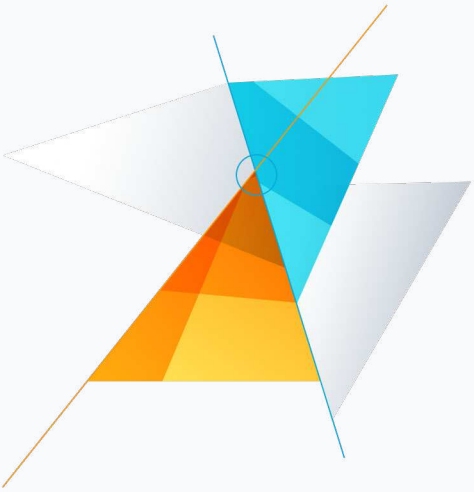
For administrator accounts, policyholders should determine if there are any free MFA solutions available for the admin credentials. This however is less likely, especially if they are a hybrid on-premise and cloud environment, and they may need to identify an MFA solution such as Duo or Okta.

For more information on MFA, visit:

- Corvus tips on implementing MFA (PDF)
- Our Knowledge Nest article on MFA

For policyholders looking to hire experts to help them implement MFA, Corvus offers an MFA Consult that can be requested via our simple form with no up-front commitment. We will then connect policyholders to vendors to assist at reduced, cost-effective rates.

Need more help? Email services@corvusinsurance.com, and be sure to copy in your Corvus Underwriter and your broker.



CORVUS

Endpoint Detection and Response (EDR)

What is EDR?

Endpoint detection and response (EDR) is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

The core functions of an acceptable EDR solution include:

- Monitoring and collecting activity data from endpoints that could indicate a threat
- Analyzing the data to identify threat patterns
- Automatically responding to identified threats to remove or contain them, and notify security personnel
- Access to forensics and analysis tools to research identified threats and search for suspicious activities

When evaluating an EDR solution, a keen eye is needed to cut through the marketing messaging. Antivirus products may appear to have many bells and whistles, but ultimately lack some of the key functions listed above. And some of the EDR software vendors offer multiple levels of their product, the basic version of which may not have EDR features and is effectively just antivirus (AV) software. When in doubt, send your Corvus Underwriter the full name of the product that you're using or considering, and we can let you know if it's a true EDR solution.

Why are policyholders required to implement an EDR tool?

EDR provides something that traditional antivirus or even more advanced "next-gen AV" cannot: "Flight Recorder" technology that tracks activity on the system before and after an alert to clearly identify what malicious activity occurred on the system. EDR can provide insight into data from all of your systems, allowing for quicker investigations and reducing the time to get up and running following an incident. Additionally, EDR carries unmatched capabilities to protect your network's endpoints. If there's a threat detected, EDR can isolate the potentially impacted system from the rest of the network until an investigator can review the system.

For more on the differences between EDR, AV, and Next-Gen AV, please read our article covering EDR on the Corvus Knowledge Nest.

What resources are available to help policyholders implement EDR?

- Contact SentinelOne through Corvus's Partner Link and receive a 30% discount with a 60 day free trial. SentinelOne works across Windows, Mac and Linux OS and is very easy to implement.
- EDR Consult — For policyholders looking to hire experts to help them identify and implement the right EDR tool for their environment, Corvus has an EDR Consult that they can request via our simple form with no up-front commitment. We will then connect them to vendors to assist at reduced, cost-effective rates.

Need more help? Email services@corvusinsurance.com, and be sure to copy in your Corvus Underwriter and your broker.

CORVUS

Backup Strategy and Process

What is required regarding backups?

Corvus will ask if the policyholder has formal processes for regularly backing up, archiving, restoring, and segregating sensitive data. Policyholders may also be asked if they are storing three (3) copies of data in two (2) different media, one (1) of which is offsite ("3-2-1 backups"). If a system goes down, the organization is only as good as their backups and the most effective security measures typically involve a layered approach.

Why are policyholders required to have solid backup strategies?

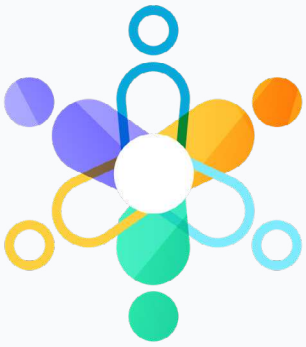
Most companies we work with during ransomware incidents have some form of backup solution or process, but all too often the backups fail due to poor security controls. Having a great backup strategy (like the 3-2-1 strategy) will help ensure that organizations don't experience complete data loss. Not only can a great backup strategy mitigate against ransomware attacks (quicker recovery, less likely to pay the ransom, etc.), it can also reduce the impact of human error, be leveraged in the event of a natural disaster, and help organizations stay compliant.

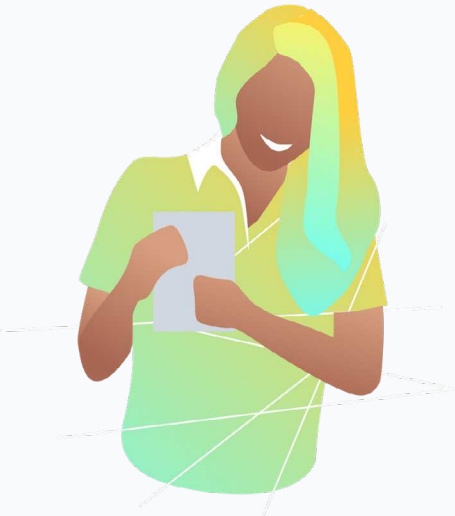
What resources are available to help policyholders strengthen their backups?

Whether by human error or cyberattack, if your system goes down, you are only as good as your backup. Below are some resources related to backup solutions and best practices.

- Learn more about the ABCs of 3-2-1 Backups on our blog and check out our detailed article here.
- Read helpful backup solutions reviews sorted by revenue size.
- For policyholders looking to hire experts to help them improve their backup strategy, they can request a backup consult through Corvus. We will then connect them to vendors to assist at reduced, cost-effective rates.

Need more help? Email services@corvusinsurance.com, and be sure to copy in your Corvus Underwriter and your broker.





CORVUS

Email Security Filtering Tools

What are email security filtering tools?

An email security filtering tool, known by security professionals as a Secure Email Gateway (SEG), is software used to monitor inbound and outbound emails to protect businesses from spam, phishing, or malicious emails containing viruses and malware. The gateway works by scanning URLs and attachments in emails for any malicious content.

With email compromise used as a common attack vector for hackers to get access to an organization network, an email security gateway can serve as a first line of defense. Not only can a SEG block and protect businesses from email threats — organizations can also utilize their email security filtering tool to meet compliance needs, thanks to email archiving and encryption features, and to potentially avoid business interruption (since some SEG providers can give users access to cloud email services should their network go down).

What resources are available to help policyholders implement email security filtering tools?

- Proofpoint
- Mimecast
- Cisco Ironport
- AppRiver
- SonicWALL

If you are using cloud-based email platforms like Microsoft 365 or Gmail, you can consider services that are in-line operation, meaning mail flows directly through the email monitoring service and it monitors traffic without having to redirect mail flow. Products like Agari offer this service. To research and find the right solution for your organization, see Gartner's peer reviews of different solutions.

If the policyholder is using Microsoft 365, then consider turning on Microsoft Defender for Office 365 to meet the requirement. Microsoft Defender for Office 365 is standard in Microsoft 365 E5 or higher but can be added to other Exchange and Microsoft Office 365 subscriptions for an additional cost.

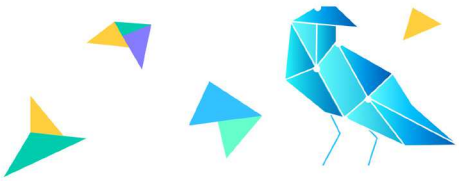
Need more help? Email services@corvusinsurance.com, and be sure to copy in your Corvus Underwriter and your broker.

Corvus Finding

The Data Science team at Corvus analyzed the rates of phishing incidents among policyholders based on the email provider/email security tool the organizations used. Policyholders using a below-average rated email security service were 2x more likely to experience a cyber claim when compared to the group using above-average email security tools.

CORVUS

Data Encryption



What is data encryption?

Data encryption is a straightforward but powerful tool to protect sensitive information from threat actors. It translates data into another form so that only people with a secret password or key can see it. Taking adequate steps at your organization to guarantee your data is protected requires that you first know where encryption is already installed, and second, recognize where you need to take actionable steps for more secure protection.

Where are policyholders required to implement encryption?

The three main components of data encryption are Endpoint Encryption, Mobile Device Encryption, and Backups Encryption.

Endpoints: Endpoints are your organization's laptops and desktops. With these devices you want to ensure that the hard drives themselves are encrypted so that stolen laptop passwords alone won't enable someone to access sensitive data. While most Mac and modern Windows devices are encrypted by default, it is best for your organization to enforce and manage the devices with a centrally managed solution.

Mobile Devices: These are cell phones and tablets used to access company resources. Like endpoints, most Android and iOS phones and tablets are encrypted by default, but implementing a Mobile Device Management (MDM) solution is a great way to further reduce risk and validate compliance.

Backups: Backup files stored on disks should be encrypted at the file level as an added layer of security in the event a hacker should access your environment through a backdoor. Cloud backups are often encrypted but it's always a good idea to confirm with your provider.

Why are policyholders required to have data encrypted?

With increasing rates of cybercrime, encryption is crucial to protect and keep personal information from threat actors. If an unauthorized party should access your environment, having strong encryption controls can protect an organization's valuable information, help you comply with industry regulations, and can protect you from any breach notification laws.

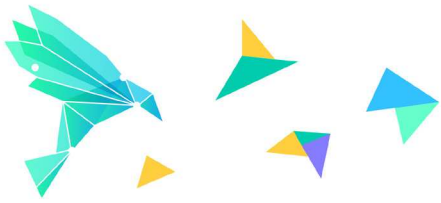
What resources are available for policyholders to implement data encryption?

- Learn more in our Data Encryption Whitepaper
- A list of the top Endpoint Encryption Software in 2021
- Peer reviews of Mobile Device Management solutions from Gartner

Need more help? Email services@corvusinsurance.com, and be sure to copy in your Corvus Underwriter and your broker.

CORVUS

Remote Desktop Protocol (RDP)



What is Remote Desktop Protocol?

Remote Desktop Protocol (RDP) is a Windows service that allows users to remotely connect to a Windows machine. More simply, RDP allows someone on remote Computer A to login to Windows Computer B as if they were physically sitting at the system. Historically, businesses expose RDP to the Internet as part of a common remote access method to enable their users to more easily access company systems and data. IT consultants also historically leveraged RDP to assess and fix their clients' systems remotely.

Why are policyholders required to properly secure or move away from use of RDP?

Threat actors commonly target external facing RDP as a primary method of gaining access to an organization's network. This is done using stolen credentials or brute forcing weak user credentials. Once an initial foothold is accomplished using RDP, threat actors will move undetected in your environment and deploy malware. This often leads to ransomware infections.

Organizations that continue to use RDP expose themselves to an increased likelihood of attack since a large number of threat actors focus efforts on breaking in using this mechanism.

What resources are available for policyholders to help secure or find an alternative to RDP?

- Learn how to secure RDP or move away from its use entirely through the RDP article on Corvus's Knowledge Nest.

Need more help or want to know additional details about the domain/IP Address where we located open RDP? Email services@corvusinsurance.com, and be sure to copy in your Corvus Underwriter and your broker.

CORVUS

About Corvus

Corvus is reimagining commercial insurance for a digital world by making insurance smarter, companies safer, and brokers more successful.

Corvus empowers brokers and policyholders with actionable insights to mitigate complex risks and reduce losses through the CrowBar digital platform, smart insurance products, and premier risk management services. Corvus is the world's largest specialty commercial InsurTech company.

Founded in 2017 by a team of veteran entrepreneurs from the insurance and technology industries, Corvus is backed by Insight Partners, Bain Capital Ventures, .406 Ventures, Hudson Structured Capital Management, Aquiline Technology Growth, FinTLV, Telstra Ventures, Obvious Ventures, and MTech Capital. The company is headquartered in Boston, Massachusetts, and has offices across the U.S.