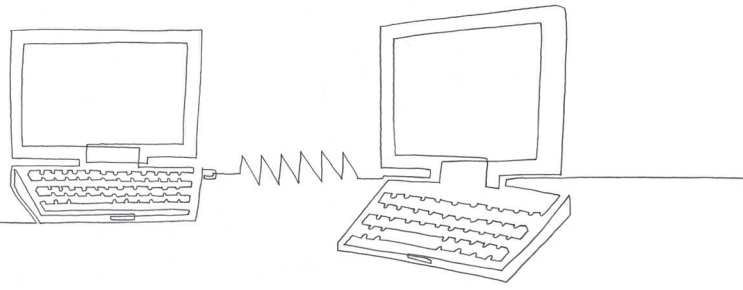
Ransomware: Best Practices for Prevention and Response

What is ransomware?

Ransomware is a type of malicious software that restricts access to an infected machine, usually by systematically encrypting files on the system's hard drive, and then demands payment of a ransom, usually in a crypto-currency (e.g., Bitcoin), in exchange for the key or keys to decrypt the data.

How can you prevent a ransomware infection?

- Audit your network for external-facing remote desktop protocol (RDP) and terminal services and turn them off where possible. If you cannot turn the services off, ensure they are patched, enable two-factor authentication, and change the default ports. Limit RDP access to only those users who have a business need for it, and secure access through a virtual private network (VPN) or Remote Desktop gateway.
- Enable strong password and account lockout policies to defend against brute-force attacks. Log and monitor RDP logins and attempted logins.
- It is a best practice to turn on two-factor authentication for external access to all applications. This is particularly true for sensitive ones such as email, payroll or benefits providers, RDP, and VPNs.
- Ensure anti-virus software is up-to-date. Use a separate password to protect anti-virus settings.
- Regularly train employees to avoid phishing attempts and not to open unsolicited attachments and links, particularly from unknown sources.
- Periodically test employees through phishing campaigns, monitor the effect on response rates, and consider a formal sanctions policy (after consultation with HR and your legal counsel) for repeat offenders.
- Block emails with .js, .wsf, and .zip extensions and macros at your email gateway level. If possible, disable the following commonly used attack vectors: Adobe Flash Player, Java, and Silverlight.
- Block macro-enabled malware files from running on Microsoft Office programs like Word, Excel, or PowerPoint by using group policy setting.
- Disable SMBv1 on all Windows systems.
- Disable Powershell on workstations.
- If you use JBoss, review the developer information on configuring and hardening it.
- Evaluate whether application whitelisting makes sense for your systems.
- Disable autorun/autoplay functionality on your operating system to prevent malicious software from running on your computer. This will prevent an external hard drive or fixed drive from automatically running a program.
- Enable automated patches for your operating system and web browser. Robust network segmentation can often reduce the impact of ransomware.
- Enable strong identity and access management, with the use of established principles of least privilege ("need to know"), and limit local administrative rights.
- Invest in an intrusion detection system to monitor signs of malicious activity. Implement (and test) a data backup and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location (preferably offline). Backup copies of sensitive data should not be readily accessible from local networks.



How can you respond to a ransomware infection?

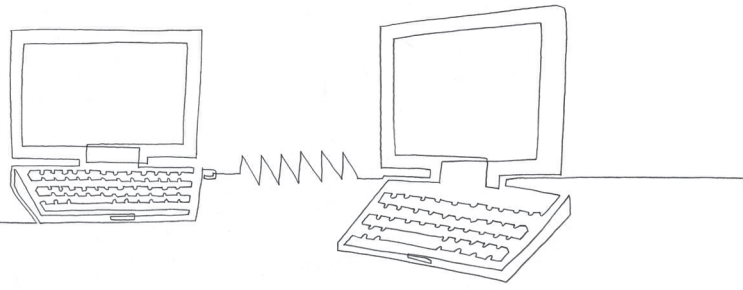
- Infected machines should be disconnected from the network (wired and wireless) as soon as possible.
- Evaluate extent of infection, attempt to identify the type of ransomware variant, and determine whether the infected machine was connected to shared or unshared network drives, external hard drives, USBs, or cloud-based storage. You may also want to check for a registry or file listing created by the ransomware.
- Evaluate whether there are any other malicious scripts or malware running on the infected machines. If so, preserve a copy of the ransomware variant and any other malicious scripts or malware for later forensic analysis to identity the capabilities of the particular ransomware variant or malicious scripts or malware.
- Clean the ransomware, malicious script or malware from impacted systems (a variety of free and paid disinfection tools exist for this purpose) and reinstall the operating system. Do your own due diligence on the tools you use. Beazley does not endorse products in any manner, but reputable tools can be found from, for example, BitDefender, Kaspersky Labs, Norton/Symantec, and Trend Micro.
- The best situation is often to restore from a reliable backup. A well thought out backup and restoration plan is one of the most important countermeasures against ransomware. It is critical for organizations to ensure that there is adequate network segmentation and/or off-line backups in place to protect your backups from corruption by the ransomware.In addition, organizations should regularly test their backup to ensure that the process is functioning as designed and there is no data corruption.
- We recommend working with a reputable security company to help prevent reinfection.

How can you respond when you don't have a backup of the data?

When unable to restore from a recent back-up or when faced with the prospect of operations grinding to a halt, many organizations elect to pay the ransom request, especially where the amount is relatively low. In doing so, organizations often struggle to procure the necessary amount of crypto-currency (e.g., bitcoin), and some thought should be given by organizations on how they would go about doing so.

The increased availability of ransomware-as-a-service and the large number of ransomware variants have made it harder for organizations to negotiate, pay, and successfully decrypt their data, so we encourage you to contact Beazley Breach Response (BBR) Services if you experience a ransomware incident.

- There is no guarantee of honor amongst thieves; the attackers might just take the money and run, or their decryption code might fail to work. There is also no guarantee that you're paying the right criminal.
- Some types of ransomware can be decrypted with the right tools. Find out what the variant of ransomware is and see if a legitimate decryption tool is available. Be cautious of companies telling you they can "break the encryption." Many ransomware variants employ commercial-grade encryption against which brute force attacks are difficult or impossible. Additionally, be careful about the source of any "decryption tool" so that you are not causing more harm by downloading another piece of malware.
- Consideration should be given to how and to what extent you should try to communicate with the criminals. Often, ransomware that comes with an extortion demand has a hotline or even webpages dedicated to guiding affected victims through the payment protocol.
- If you intend to communicate with the criminals, set up an anonymous email account for that purpose. Do not provide any additional information about your organization; doing so could lead to an increased ransom demand.



- It is possible to negotiate a lower price with the criminals, as well as to ask them for additional time to pay to buy yourself time.
- Keep in mind that it is possible that the criminals have no idea what type of data is at risk, nor do they usually know the status of your backups. Do not share any type of identifying information with them. If they find out your data is very sensitive, the ransom demand could jump significantly.
- Some types of extortion arrangements come with a "proof of life" which can help you verify that the criminal has the ability to unlock your files.
- Thoughtful consideration and caution should be used if you are accepting any file from these criminals. Any decryption keys or "proof of life" could contain additional malware.
- Purchasing bitcoin online can take up to 3-5 business days in some cases. Typically you can purchase bitcoin from an exchange or broker. Reputable U.S. based exchanges require payment by ACH bank transfer, which takes a few days.
- It is possible to speed up the process by using a credit card or debit card at an exchange based outside the United States, but the risks are greater. Not all exchanges are trustworthy. Even if the exchange is reputable, these types of sites usually charge a larger premium for the transaction because of the high risk of fraud.
- If the bitcoin amount is relatively low, obtaining bitcoin from a physical ATM may be the quickest option. A network of physical Bitcoin ATMs exists in most major metropolitan areas where bitcoin can be bought in person.
- In order to use purchased bitcoins, you have to establish a bitcoin wallet. The various types of wallets include the following:

  Online bitcoin wallet - access from the web
  Hardware bitcoin wallet - a physical bitcoin device you own
  Software bitcoin wallet - an application installed on your computer or mobile device
  Paper bitcoin wallet - physical paper with your private key

- As your trusted insurance carrier, we cannot provide any assurance or guarantee that any one exchange, wallet, or bitcoin transaction can be completely trusted. We also cannot provide you assurance that your transaction will result in data recovery.

I have the bitcoin and wallet and I am ready to pay

A few things should be considered here. Are you OK with paying an unknown source? Are there any compliance or legal considerations involved in using your organization's funds to pay a ransom payment or make a payment to an unknown sources?

- Any files received from the criminals should be scanned for malware.
- Consider testing the decryption key on a backup of the encrypted data if possible so that you can see if it works without potentially causing a data corruption issue with your encrypted data.

This all sounds too complicated. Can Beazley help?

Absolutely. We recommend that before considering payment of any ransom you contact Beazley Breach Response (BBR) Services. We will also walk you through your options and potential vendors that can help at every step of the way, when possible.

We maintain a list of service providers that are readily able to assist our insureds when they have a ransomware incident. Services may include identifying the ransomware variant and capabilities, negotiating a ransom demand, confirming "proof of life," making a ransom payment, assisting with decryption, and conducting a forensic examination to determine if any sensitive data was accessed or exfiltrated.

You can contact BBR Services at bbr.claims@beazley.com or by phone at 866 567 8570.