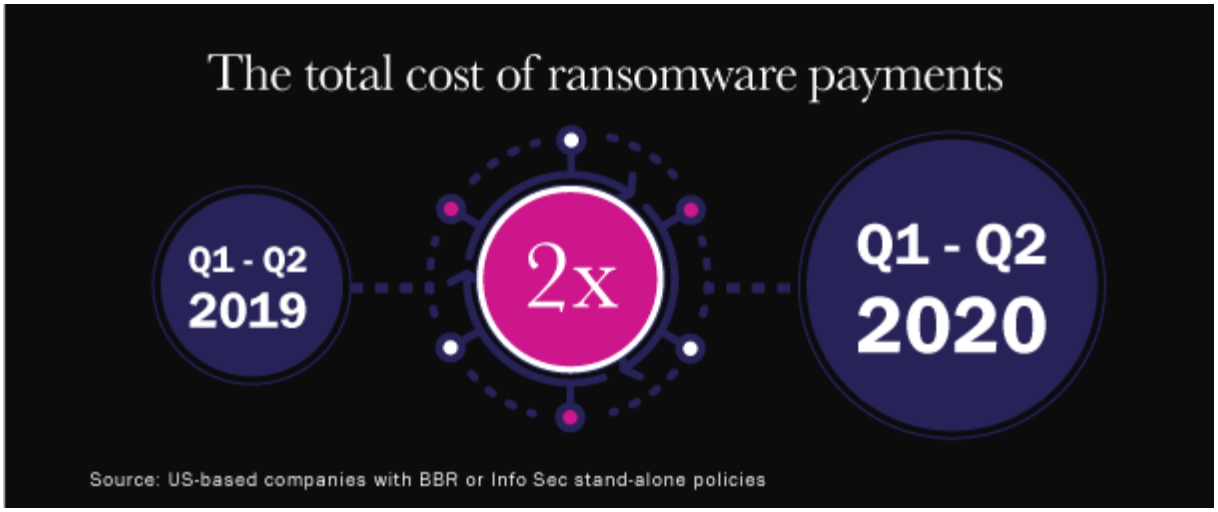
Beazley Breach Insights - Q3 2020

Increasing severity in ransomware calls for layered cyber defenses

In an incredibly challenging year in which ransomware has easily become the biggest cyber threat to impact individuals and organizations alike, the severity of ransomware attacks has continued to escalate. During 2020, these incidents have reached new levels of complexity, having developed a long way from the early incarnations of ransomware designed to trick an employee into clicking on a bad email that then encrypts a workstation and file shares. Today's cyber extortion events are much more likely to involve threat actors who exploit access into networks, install highly persistent malware, target backups, steal data, and threaten to expose the compromise. As the criminals become more sophisticated, it is more important than ever for organizations to adopt a layered approach to security, and take stringent measures to stop or minimize a cyber extortion event at every stage.

Beazley Breach Response (BBR) Services projects the frequency of ransomware incidents in 2020 is oscillating between the higher end of the range seen in 2019. Despite the fluctuation in the number of incidents, BBR Services reports a rise in severity as incidents reported are more complex.



Cyber extortion more often includes a threat to release stolen data

Threat actors increasingly have prior access to a network before deploying their attack, during which time they are working to escalate their privileges, move laterally through the network, and perform reconnaissance on the network and data stored on it. Frequently, they are now also exfiltrating data and uploading it to an external site, both to prove that they have access and to threaten exposure. According to data from ransomware incident response firm Coveware, almost 50% of ransomware cases in Q3 2020 included the threat to release exfiltrated data along with encrypted data, up from 22% in Q2.

In one recent example, BBR Services assisted an automotive group hit with eGregor ransomware after the ransomware encrypted servers hosting personally identifiable information (PII) for employees. Backup

systems were compromised as well. The initial contact with the threat actor was with the automotive group's IT provider and the cyber extortion demand was set at nearly $500K. The threat actor provided proof they had exfiltrated employee data. With Beazley's assistance, the company engaged privacy counsel, forensics, and a ransom negotiator. Forensic investigation revealed the infection vector was likely a malicious email sent from a compromised email account outside the organization. Over the course of several days, the ransom negotiator succeeded in lowering the demand to $50K. Because their backups were compromised, the automotive group made the decision to pay the demand. The threat actor provided the decryption key and confirmed deletion of exfiltrated data, and the automotive group was able to decrypt their data and return to normal operations.

In this incident, the threat actor had exfiltrated employee data, but not customer data, which was protected on a separate platform. Companies that fear that the exposure of stolen data may embarrass them need to think hard about whether that is a reason to pay a demand. One consideration is that if the stolen data involves PII or protected health information (PHI), they may already have a legal obligation to notify affected individuals. Another is that different threat actor groups can be involved in different stages of the process, which can increase the possibility of re-extortion. Often one threat actor has compromised the network and sold that access on the dark web. A different threat actor exploits the access for cyber extortion, but other groups may also have access to the data. Finally, there is no certainty that the threat actor will keep up its end of the bargain. As Coveware reports, in some cases stolen data has been posted before the extortion demand was paid, and in others the threat actor has re-extorted the victim organization weeks later.

Organizations need to make it hard for threat actors at every step

Cyber extortion is a process and there are many opportunities along the way to disrupt the criminals' activities. Ransomware is avoidable but requires regular and thorough training of employees on how to avoid this evolving threat. Organizations should not only try to prevent a ransomware infection, but prepare in case they do get infected,

through multiple layers of security, each reducing the risk and probability of ransomware. Training employees to recognize phishing emails; establishing secure, offline backups; encrypting data at rest; monitoring for network intrusions; keeping up with patching systems and applications—all of these make it harder for an attacker to exploit access even if they do get into a network.

Steps to protect against ransomware

1. **Start with a risk assessment.** Addressing risks starts with identifying what they are, where they are, and how severe the consequences are.
2. **Email content and delivery:** Enforce strict Sender Policy Framework (SPF) checks for all inbound email messages, verifying the validity of sending organizations. Filter all inbound messages for malicious content including executables, macro-enabled documents and links to malicious sites.
3. **Manage access effectively:** Ransomware doesn't have to go viral in an organization. Put in place appropriate measures for general user and system access across the organization: privileged access for critical assets (servers, end-points, applications, databases, etc.) and enforce multi-factor authentication (MFA) where appropriate (for example remote access/VPN, externally facing applications).
4. **Back-up key systems and databases:** Ensure regular back-ups that are verified and stored safely offline. Use strong, unique back-up credentials, and secure them separately. Test backups to ensure restoration from them.
5. **Educate users:** Most attacks rely on users making mistakes. Train users to identify phishing emails with malicious links or attachments. Regular phishing exercises are a great way to do this.

6. **Patch systems and applications:** Conduct regular vulnerability scans and rapidly patch critical vulnerabilities across endpoints and servers – especially externally facing systems.
7. **Secure remote access:** Do not expose Remote Desktop Protocol (RDP) directly to the Internet. Use Remote Desktop Gateway (RDG) or secure RDP behind a multi-factor authentication-enabled virtual private network (VPN).

Additional resources on Beazley's 360 approach to ransomware and suite of cyber services https://www.beazley.com/usa/cyber_and_executive_risk/cyber_and_tech/beazley_breach_response/cyber_services/cyber_extortion_us.html.

BBR Services – a dedicated team of experts

Beazley is unique among insurers in having a dedicated business unit, BBR Services, that focuses exclusively on helping clients manage cyber incidents successfully. This in-house team of experts works closely with cyber policyholders on all aspects of incident investigation and breach response and coordinates the expert services that insureds need to satisfy legal requirements and maintain customer confidence.

In addition to managing data breach response, BBR Services provides a full range of resources to help mitigate risks before an incident occurs. BBR Services develops and maintains Beazley's risk management portal as well as coordinates newsletters and live expert webinars and pre-breach services such as onboarding calls, incident response plan reviews and on-site workshops.