Texas Council
Risk Management Fund

Ransomware Protection Measures

Ransomware attacks are increasing in frequency, and the repercussions are growing more severe. Ransomware attacks cost companies billions of dollars a year. Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the WannaCry malware attack in 2017. An overwhelming majority of ransomware attacks now include a threat to publicly disclose stolen data if the ransom isn't paid. This adds a second level of extortion as an attempt to guarantee that the ransom is paid.

Protecting against ransomware attacks requires an approach that combines security defenses with proactive measures to prevent ransomware from taking hold in the first place. Here are five protection measures.

Perform regular system backups

Seen as the backbone of ransomware recovery, system backups don't provide as much protection as they once did due to second level of extortion. Additionally, many next-generation ransomware attacks find and destroy backups. However, secure backups still play a vital role in restoring systems after a ransomware attack, as well as hardware failures and natural disasters. Utilize at least two different backup methods, each stored at a different location.

Conduct regular network and security assessments

Most compliance standards entities call for organizations to perform penetration tests and vulnerability scans at certain intervals. Typically, they require organizations to run vulnerability scans quarterly and perform penetration tests annually. However, these are the bare minimum requirements. There are many circumstances under which more frequent scans or penetration testing are warranted, such as whenever organizations make a major change to their data environment. Many insurance companies providing cyber risk policies will conduct their own scans and assessments in an effort to gauge potential risks with the client. Conducting regular assessments could help to stay ahead of the cyber insurance world and mitigate premium increases.

Segment your network

Network segmentation, which involves piecing out a larger network into smaller segments using firewalls, virtual LANs, and other techniques, doesn't prevent cyberattacks from happening. However, it does stop malware or human intruders from moving laterally within your network — a key factor in double extortion ransomware attacks. Cybercriminals can't upload what they can't access. Segmenting is typically done by function, such as separating public-facing services from internal applications, or by data type, such as separating user workstations from servers.

Increase your password security
Even before remote work became widespread, a majority of data breaches were due to compromised passwords. As remote work exploded in popularity, brute-force attacks targeting remote desktop protocol (RDP) connection credentials rose exponentially. The majority of ransomware attacks now involve either RDP credential compromise or phishing — in other words, compromised passwords. Organizations need to implement robust password security protocols, including requiring employees to use strong, unique passwords for every account and enable multi-factor authentication (2FA) whenever it's supported.

Conduct employee security training
It happens every day: High end security technologies are defeated because an employee clicked on a phishing link. Just as employees who work in industrial environments must undergo safety training to operate machinery, network computer users must be trained to operate computers safely. Because the cybersecurity threat environment is always changing, employee cybersecurity training should be viewed as continuing education. Organizations need to regularly conduct simulated "phishing attacks" to gauge employee awareness and knowledge. Employees also need to know who to contact, and how to get in touch with them, if they encounter a security issue or have a question.