



Solutions

Managed IT

Could your business survive a ransomware attack? Ransomware is no longer rare, it's now the most common form of cybercrime, and it's costing organizations several thousand dollars in recovery. In this blog, we outline three essential steps to protect your business before it's too late. With the right strategies and the right partner, you can build a rock-solid defense. Don't wait for a breach to take action. Learn how to safeguard your business today.

Fight Back Against Cyberattacks

What used to be a rather rare occurrence has now become the single biggest type of cybercrime today. Ransomware is a cyberattack in which computer systems are held hostage by hackers demanding payment. In 2020 alone, 2,354 government entities, healthcare organizations, and schools across the nation became victims of ransomware attacks, and at one point, the average payout surged to \$178,000! As cybercrimes such as Ransomware continue to skyrocket, we're sharing tips for how to prevent and protect your organization against cyberattacks.

1. Backup all critical information.

This one simple step could be your saving grace when disaster strikes. Scheduling automatic backups will ensure that you always have access to current data in the event of a natural disaster or cyberattack. Taking the time to back up your files now will save you time and money later by reducing downtime and recovery time. Systel can help you identify a strategy that is customized to your business, and will automatically ensure that you have a solid business continuity plan.

2. Complete a risk assessment.

Ransomware is the fastest growing malware threat, targeting users of all types, whether at home or on the business network. When taking the steps to protect your organization, you must first identify threats and vulnerabilities in your business's network. Network vulnerabilities are weaknesses or flaws in software, hardware, or organizational processes that when compromised by a threat, can result in a security breach. Using the Network Check-UP tool, your network will be assigned a Risk Score based on impact, and as a result, we can provide recommended fixes and track the remediation process from start to finish, giving you a better understanding of how to prevent and protect your network from external threats before it's too late.

3. Invest in Cyber Insurance.

Aside from physical risks like property damage and work injuries, your business is prone to damages that result from everyday technology use. A majority of organizations process and store confidential data digitally, including the names, addresses, social security numbers, medical records, and banking information of employees and customers. Data breaches compromise not only the safety of personal information, but also the integrity of your organization. Systel offers cyber insurance to help mitigate first and third party losses that result from cybercrimes, in addition to providing preventative resources and end-user training on cybersecurity best practices.

FIND THE RIGHT FIT BY PARTNERING WITH SYSTEL

Systel's Managed Services Specialists are highly skilled and trained in their area of expertise. We aim to improve your business's day-to-day operations through our host of products and solutions that are customized to your individual needs. Don't get caught off-guard. Investing in a continuity plan now can save you years of headache and astronomical recovery costs. Let Systel help you find the right fit for your needs. [Contact us](#) today for more information.