WE MAKE CYBER SIMPLE

RANSOMWARE - EVERYTHING YOU DO MATTERS

Ransomware has progressed from an annoyance to a major scourge. The attackers are getting more adept at finding ways to infiltrate your environment to install their malware.

After a successful ransomware attack you have two choices, pay the ransom or don't. Paying the ransom will hopefully get you a working decryption key. But don't count on it. Companies who paid the ransom only recovered 61% of their data on average, and only 4% recovered all their data.

Choosing to not pay the ransom means restoring everything from a current unencrypted backup, which takes time.

To discourage this, attackers steal your information before encrypting and threaten to reveal or sell it if you don't pay. Even without the threat of having stolen data released, the cost of a full restoration from backup is not cheap, $1.85 million in 2021, almost double 2020.

So, what do you do? As with any significant business challenge, planning is essential. Planning needs to cover the five stages of good cyber protection: Risk assessment, Enhance your protections, Incident response, Recovering from an incident, and Support afterwards.

Risk assessment examines your current situation and identifies the risks you face and prioritizes them. Enhance your protections uses the risks to determine the best approach to mitigating them. This is 3-pronged; Planning what needs to be done, Training to improve awareness, Protecting by implementing what was identified in the prior stages.

Incident response creates the plan for what to do, and not do when an attack succeeds. Creating the plan in advance is absolutely essential. Being the victim of a cyberattack is stressful enough. It is not the time to create the plan. Also necessary is a Communications Plan to know who to contact and have their contact information.

Ransomware can be made much worse by taking actions without the proper knowledge. Regulators, law enforcement, and cyber insurers have certain requirements in the event of a cyber incident. Failing to meet those requirements may leave you open to fines and denial of a cyber insurance claim.

Recovery starts after Incident Response to return you to the state before the incident.

Support takes a look at what happened and what can be done to improve your protections and hopefully prevent a recurrence.

Without a complete plan you are leaving yourself vulnerable and jeopardizing your company.

We can provide a ransomware service that meets your industry needs and fits your budget. We have been helping companies for years and are ready to help you. See why we say We Make Cyber Easy!

Ready to take the next steps? Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.