Once you've been hit, your business is never the same

In additional to financial costs and reputational damage, a ransomware attack can also lower the confidence of your IT security team.

Being hit with a ransomware attack damages an organization in many ways – from stopping it being able to fully operate for weeks, to angry customers and potential reputational damage. However, a ransomware attack also has a human cost, affecting the confidence of IT and information security teams – and potentially for a long time after the initial attack.

A new research paper by cybersecurity company Sophos says the extent of this confidence hit is so significant that the culture at these companies is never the same again. That's perhaps not surprising as there are some suggestions that suffering a major attack can make your organization more likely to be hit again because criminals will identify it as a company that could be an easy target.

According to the survey, nearly three times as many IT and information security staff in organizations that have been hit by a ransomware attack feel as if their organization is 'significantly behind' when it comes to facing cyber threats, compared with those in organizations that haven't suffered a ransomware attack. That lack of confidence also extends to business leadership, where management of a company hit by ransomware will also perceive the company to be significantly behind on cyber threats, compared with companies that haven't.

More than one-third of ransomware victims said that recruiting and retaining skilled IT security professionals was their single biggest challenge when it comes to cybersecurity, compared with just 19% of those that hadn't been hit. Being hit with a ransomware attack also appears to have an impact on re-skilling and training employees, with the results of the survey suggesting that organizations that have fallen victim to a ransomware attack are more likely to implement 'human-led' threat-hunting on their networks over those that haven't been hit.

The idea is that by having human eyes on the network, it could be easier to spot unusual activity that could be the hallmark of an incoming cyberattack. This could prove to be important for organizations that have fallen victim to ransomware attacks that could also find themselves more vulnerable to additional cyber threats following an incident.

However, despite the number of organizations that have fallen victim to cyberattacks, the report concludes that it's "encouraging" how information security teams are evolving, especially when it comes to reacting to ever-evolving threats.

If your organization is unable to provide an information security staff, we suggestion looking into the implementation of an outside resource, such as the Managed Network Services team from CDS Office Technologies. CDS will provide the most advanced and cost-effective solution for monitoring, controlling and updating your IT security environment.

www.cdsot.com 1-800-367-1508