The Horrors of Ransomware

Ransomware Equals a Data Breach

From a data regulator's perspective, it is the responsibility of your business to keep data safe from cyberthreats, inform clients about a breach within a stipulated period and provide necessary documentation as proof of your efforts. Although different regulations have laid down distinct mandates for breach notifications, the principle remains intact.

While there is an over-arching belief that data isn't really "stolen" in a ransomware breach, no organization hit with ransomware has been able to back this up as fact. That's why compliance regulations mandate businesses to notify their clients if their data is in jeopardy. Many businesses, however, tend to operate in something of a "grey area" when it comes to notifying their stakeholders about data breaches. In this blog post, we'll tell you why going down this route can backfire and why your business needs to adopt an inclusive approach that combines the best of cybersecurity and compliance.

The grey area

Many businesses seem to think that not all ransomware attacks need to be reported since not all hackers can decrypt the data they have encrypted themselves. They assume that only during sophisticated attacks do hackers possess the necessary skills to decrypt, exfiltrate and misuse data. Only in such cases do these businesses accept that a breach has occurred and is, hence, in need of reporting.

However, this assumption is dangerous for two reasons. First, with enhanced ransomware-as-a-service tools readily available in the market, even a hacker with minimal skills can catch you off guard and wreak havoc. Second, regulatory agencies perceive the situation differently.

For example, as per HIPAA's Privacy Rule, the U.S. Department of Health and Human Services has advised companies to assume that ransomed data contains Personal Health Information, even in "low probability" cases. In fact, some data breach notification regulations mandate businesses to notify customers even in the case of "unauthorized access," without the need to prove that personal data was stolen.

Why businesses choose silence over breach notification

Accepting a data breach isn't easy for any business due to the severe financial and reputational repercussions. But there are other reasons why businesses choose to keep quiet.

Inability to comply with data breach notification norms

Despite being a basic requirement, most businesses lack the ability to adhere to breach notification norms set by several regulations worldwide. Even if a business avoids reporting a ransomware attack, failing to notify its customers or clients on time can still invite stringent action from regulators.

GDPR — the European Union's data privacy and protection regulation — has set a 72-hour deadline to report the nature of a breach and the approximate number of data subjects affected. From the moment a business' IT team establishes that a breach has occurred, the clock starts clicking.

Is your business capable of adhering to such norms?

The "victim versus victimizer" perception

Let's assume a business reported a ransomware breach to its stakeholders and the relevant authorities. On one hand, law enforcement agencies investigating the matter would perceive

the business as a victim, even if it paid the ransom; on the other hand, regulators might deem the business to be the victimizer of its customers for failing to protect their data.
If the business is found to be non-compliant with the necessary security mandates after an audit, the regulators will undertake punitive action after assessing a list of factors.

Reputational damage

Most customers prefer not to engage with a brand following a data breach. Who would like to associate with a business that can't protect itself?
While your business could still recover from the financial damage caused by ransomware-induced downtime, rebuilding its reputation and regaining the trust of your customers is a long, tedious and more often than not, futile process. This is one of the main reasons why businesses abstain from reporting a ransomware breach.

You need to cover both ends

While there isn't a 100% fail-safe strategy to avoid cybersecurity attacks such as ransomware, your business can still demonstrate its commitment to preventing security breaches or data loss incidents. This is just what compliance regulators, as well as your key stakeholders, look for — how proactively your business can mitigate risk and handle the aftermath of a breach while also adhering to applicable regulations.
Adopting an inclusive approach that involves the best of cybersecurity and compliance is a step in the right direction. Partnering with an experienced MSP that has a track record of protecting businesses from sophisticated cybersecurity threats and non-compliance risks will significantly benefit your business.

Feel free to contact us for a consultation today. Let us help you proactively meet all your cybersecurity and compliance needs. Call Tim at (717) 912-4796 Ext. 202