Regulations & Ransomware: A Quick Overview

SEPTEMBER 2021

As cybersecurity threats continue to evolve, ransomware has recently come into focus as one of the more prominent and challenging types of attacks to deal with. Not only do companies need to face the security implications of having their data fall into the hands of cybercriminals, but there can be significant costs around paying ransoms and/or recovering systems and files.

What Is Ransomware?

Before diving into what to do about ransomware and what regulations to follow, it's important to understand what ransomware is.

"Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption," explains the U.S. Cybersecurity & Infrastructure Security Agency (CISA).

In other words, ransomware can lock a user out of their own files/systems, which can bring work to a halt. Even if the ransom is paid and everything gets unlocked, it's possible that the cybercriminals stole data meanwhile.

While some of the more headline-grabbing attacks have been at large, well-known companies, ransomware can essentially affect anyone, regardless of size, industry or location.

How to Reduce the Risk of Ransomware

Although ransomware is on the rise, there are still several steps organizations can take to reduce the risk of a ransomware attack or at least mitigate the damage.

"As with all risks posed by external actors, the likelihood that a ransomware attack is successful can be drastically reduced by tightening the security of the data controlling environment," notes the European Data Protection Board (EDPB).

From updating software and systems with appropriate security patches, to using anti-malware software or related monitoring services, there are many cybersecurity best practices that can potentially keep ransomware out, as the EDPB highlights.

If ransomware does take hold, having complete backups can help. As the EDPB notes, the impact of ransomware "could effectively be contained," by resetting systems to wipe out the ransomware and then "fixing the vulnerabilities and restoring the affected data soon after the attack."

Organizations can also get a better handle on ransomware risk via cyber risk quantification (CRQ), such as through Kovrr's insurance-validated risk models. CRQ works by analyzing factors such as past cyber events and the technologies and service providers that a company uses to then quantify what companies might lose if a cyber attack like ransomware occurs. Part of being prepared means knowing how much is at stake financially, and CRQ can help organizations focus on the areas that present the largest financial risk.

What Ransomware Regulations Exist?

Current ransomware regulations differ around the world, so the specific rules an enterprise needs to follow depends on factors like what markets they operate in and whether they fall under certain jurisdictions.

Communicating Attacks

One of the more notable rules that relates to ransomware is the EU's General Data Protection Regulation (GDPR), which can still apply to companies outside Europe, such as those that have customers in the EU. Under GDPR, explains the EDPB, a personal data breach needs to be reported to relevant authorities and potentially to the people whose data gets exposed.

So, for example, if a ransomware incident involves a cybercriminal locking up files that contain personal information, such as financial or medical records, then the affected company may need to report that to those affected.

In the U.S. the rules aren't necessarily as strong. But a publicly traded company, for example, may need to report cyber attacks and risks if they're considered to be material, as the Securities and Exchange Commission notes.

Respecting Sanctions

One complication with ransomware is that paying the ransom could be sending money not just to any cybercriminal but to an individual or nation that's facing sanctions.

"Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations," explains the U.S. Office of Foreign Assets Control (OFAC).

Even if someone doesn't know that they're paying a ransom to an individual or an organization that's facing sanctions, they could still be breaking the law. Those affected by ransomware can contact OFAC if they think a ransom might affect sanctions.

Starting to Form Protections

In Japan, the Basic Act on Cybersecurity aims to lay a groundwork for cybersecurity protections. For example, the law asks critical infrastructure companies to proactively implement cybersecurity measures on a voluntary basis, as well as to cooperate with government authorities as needed, explains The International Comparative Legal Guides (ICLG).

This law first came to be in 2014 and was amended in 2018 to help the country prepare to host the Olympics. The amendments include having the government "set up a council that discusses the promotion of cybersecurity measures. The council will consist of national government agencies, local governments, critical information infrastructure operators, cyberspace-related business entities, and educational and research institutions," as the U.S. Library of Congress notes.

What Ransomware Regulations Might Be in the Pipeline?

Given the increase in ransomware attacks, many governments are considering additional regulations that enterprises need to keep an eye on.

For example, as Bloomberg Law reports, some considerations in the U.S. include banning ransomware payments entirely, as well as requiring companies to share information involving attacks. Companies may also have to implement stronger cybersecurity measures, such as using multi-factor authentication and patching software.

In the EU, reports the Wall Street Journal, critical infrastructure companies, including energy and electricity businesses, may also face stronger requirements, following high-profile ransomware attacks around the world, such as one on the Colonial Pipeline in the U.S. For example, electricity companies may need to do more to assess their cybersecurity risk.

The details of what's to come regarding ransomware regulations differ by region and in many cases still remain somewhat unclear. But the overall trend is toward more cybersecurity preparedness and potentially sharing more information among authorities.

In the meantime, enterprises can take matters into their own hands to quantify their cyber risk more precisely. Get in touch with Kovrr today to see how our cyber risk modeling capabilities can help you determine what's at stake.