Ransomware on the Rise: Preventing and Responding to a Cybersecurity Crisis

The threat of ransomware is becoming increasingly worrisome for Latin American corporations and governments. Organizations in Brazil are at an especially high risk, as the country represents the highest share (nearly 50%) of Latin American targets attacked using ransomware. While ransoms average around $170,000, they can reach into the tens of millions. The overall cost of such an attack—across regulatory fines, reputational damage, recovery efforts and legal proceedings—is usually far greater than the payment alone.

The most recent Cost of a Data Breach report from Ponemon Institute and IBM found that between 2019 and 2020, Brazil had the highest increase in the total cost of a data breach among all countries studied—with the average increasing by 29%. The study also found that remediating an incident in less than 200 days saves an average of $1.1 million. Given that Brazilian organizations typically take longer to respond than organizations in most other countries, at an average of 380 days compared to the U.S. average of 237 days, the need for improved ransomware readiness and incident response is clear.

Ransomware Readiness and Prevention

In these crisis scenarios, an ounce of prevention truly is worth a pound of cure. The extent of preventative measures an organization has taken, and the speed at which an incident is identified and remediated, are directly linked to the likelihood of ransomware attack, how costly it will be and how quickly the organization can recover.

To mitigate the risk of a ransomware attack and become crisis ready, organizations need to address the following critical elements:

1. **An effective information security program** that encompasses incident response planning, responsibilities and recovery procedures that can be followed at all times, especially in crisis scenarios. Technical and administrative policies and controls should be updated to account for the threat of ransomware, so such an attack can be detected and addressed quickly. The plan should also address the organization's agreed upon position for whether, when and under which circumstances ransoms may be paid, as well as who would pay (i.e., the company or a cyber insurance provider) and how cryptocurrency payments would be facilitated.
2. **Robust cybersecurity tools and resources.** Cyber threat and regulatory landscapes have evolved to the point at which cutting corners on security leaves organizations extremely vulnerable to an attack. A strong defensive stance against ransomware must include sophisticated technology, processes and expertise working in tandem to keep information secure. Organizations must invest in external threat intelligence, structure technology so that it meets their unique needs, keep tools up-to-date and maintain multi-tier patching strategies. A bench of trusted experts and advisors should also be at the ready to help bridge security gaps and lead investigatory and communications efforts if an incident occurs.
3. **Tailored recovery strategy and architecture.** Business continuity is paramount in reducing the risk and impact of a ransomware attack. This requires effective back-up strategies and disaster recovery plans so that operations can be reinstated from scratch if a cyber attack paralyzes existing systems and information. Data mapping and prioritization are central to recovery—with a detailed, prioritized data map that documents internal system architecture, data flows and sensitive data footprint, an organization can prioritize back-ups, disaster recovery plans and data protection controls.
4. **Comprehensive training, awareness, communications.** Technology and policies must be layered with support from every person within the organization. Security and compliance teams should work with strategic communications and change management experts to set a tone for a strong culture of security and trust. Against this backdrop, security training, simulation exercises, awareness campaigns and crisis communications plans can be rolled out to setup a resilient first line of defense against attacks.

Responding to Ransomware

If an organization is hit with ransomware before a readiness strategy has been implemented, or if an attack occurs in spite of preventative measures, rapid coordination across cybersecurity incident response, investigation, legal and strategic communications is critical. When essential systems are compromised or sensitive data is at stake, every second counts. The first step is ensuring the matter is escalated to all key stakeholders across IT, security, executive leadership, legal and communications. With a response team assembled, stakeholders should be prepared to:

- Launch a forensic investigation to begin determining what happened, what information was compromised and what steps need to be taken to contain the damage.
- Revert to the incident response plan to determine who to notify and when, and the extent of information to be shared publicly and/or with authorities.
- Initiate the business continuity plan to get operations back up and running as quickly as possible.
- Evaluate what is known about the attack—including the extent to which operations have been interrupted and whether sensitive information is at stake—to inform decisions about whether or not to negotiate with the attackers and/or pay the ransom.
- Issue transparent communications, as regulators and insurance companies will scrutinize the nature of an organization's communications with employees, affected individuals, partners, etc., in the aftermath of an incident. Clear communications also play a key role in rebuilding public trust after a data breach or cyber-related service disruption.
- Create a feedback loop so that information and vulnerabilities revealed during the investigation can be leveraged for future threat intelligence and improvement of the overall information security program and incident response plan.

Continuous Security Improvements

Knowing how to respond to a ransomware attack is vital, as the ultimate cost will largely depend on how prepared an organization was beforehand. The strongest cybersecurity

programs are created proactively and upheld by stakeholders with expertise in information security threats and best practices, as well as the key legal, regulatory and communications challenges that come into play during an attack or breach. When supported by experienced and coordinated teams, cybersecurity programs can withstand the impact of a ransomware attack and continually improve alongside a rapidly evolving threat profile.

Antonio Gesteira
FTI Technology

Jordan Rae Kelly
FTI Cybersecurity

Adriana Prado
FTI Consulting Strategic Communications