Lodestone

How to Stop Ransomware

As cybercrime expands into new realms, senior leaders from small-town school districts to Fortune 50 companies are looking for better ways to protect priceless data and fend off ransomware attacks. Many organizations are now paying small fortunes to vendors making outlandish promises—even before taking relatively simple and inexpensive steps to prevent ransomware infections and respond effectively to those that do occur.

Despite what some vendors claim, no application, computer or security system can be perfect—they're all made by humans. We recommend that every organization build a layered approach to security, update it diligently and stay vigilant to keep pace in the relentless struggle against cybercriminals.

Senior leaders should begin with a clear understanding of their IT infrastructure, who uses it and how they use it. Based on that knowledge, they can adhere more closely to best practices in their industries, whether they're retail merchants, hospital administrators, financial managers or military contractors. Indeed, many companies are required to meet strict security standards, such as the EU's General Data Protection Regulation or the California Consumer Privacy Act, but complying with regulations does not guarantee security—the rules don't always advance as quickly as the threats, and many compliant companies have been breached.

Senior leaders should begin with a clear understanding of their IT infrastructure, who uses it and how they use it.

The good news is that most information security standards and frameworks are available for free or a one-time fee, and most experienced risk and technology officers can conduct their own self-assessments before bringing in auditors, giving their organizations insights into what needs to be addressed.

HOW TO RESPOND TO A RISK ASSESSMENT

Once they have a keen understanding of the specific risks they face and where the organization is most vulnerable, senior leaders can begin to craft a robust vulnerability management program.

This is where many companies and governments struggle the most: translating assessed risks into actionable remediation efforts. Industry terminology doesn't help. Is a "firewall" an open-source tool with a simple set of rules about which ports

are open, or does it harness machine learning and other next-gen technology? The answer might depend on which vendor is providing the counsel.

For simplicity, it can help to consider three categories of security: people, processes and technology. How people and processes are related to security is well understood, so we will focus here on the four main goals of technology:

- **Avoiding compromise.** All ransomware infections start with an initial "compromise", either through vulnerabilities in the internet or human weaknesses that can be exploited through social engineering, such as phishing.
- **Preventing exploitation.** Using a compromised computer, the ransomware spreads through the organization, capitalizing on vulnerabilities across internal business networks.
- **Detecting anomalies.** At some point, the organization recognizes that it has been infected with ransomware—defenses are triggered, employees notice or attackers demand ransom.
- **Responding to events.** How quickly and adequately an organization responds to an infection determines how much damage the ransomware can inflict.

Making progress in each category requires a range of information security disciplines that we will discuss in upcoming "How to Stop Ransomware" articles. But progress begins with prioritization.

MAINTAINING PRIORITIES AS THREATS EVOLVE

As organizations learn what they need to accomplish to improve security, they quickly realize that they can't do everything at once. We recommend using a four-step process to draft a roadmap: categorize risks and rewards; identify the human and technological resources available to close gaps; set priorities; and launch programs.

CATEGORIZE RISKS AND REWARDS

Risk and vulnerability assessments, penetration tests and so on provide empirical, technical data about risks, their severity in relation to best practices or regulatory standards, and actual business risks.

Approaches to quantifying business risk vary widely, but we start with basic questions like these:

- Based on the risk assessment, where are the weakest areas in your organization?
- Which risk categories are most important—financial, reputational, regulatory, competitive?
- What risk-reduction initiatives would deliver the most value for your organization?

Comparing resources with potential security gaps, we help clients determine whether they need new training programs, short-term contractors or full-time hires for the long term.

IDENTIFY RESOURCES

We ask clients how many employees are dedicated to security and IT, what skills they have, what technology and software is in place to address identified risks, and how much room they have in IT and IS budgets to acquire additional human or tech capital.

Comparing resources with potential security gaps, we help clients determine whether they need new training programs, short-term contractors or full-time hires for the long term.

PRIORITIZE ACTIONS

Based on the resources they have and can acquire, IT and IS leaders can set goals for the next week, month, quarter and year. The most useful roadmaps include detailed, tangible deliverables and deadlines that senior leaders understand and support.

A good roadmap also identifies everything that could affect day-to-day operations, including delays and bottlenecks. In our experience, “fire drills” are almost certain to cause delays. People should be prepared for them.

The most useful roadmaps include detailed, tangible deliverables and deadlines that senior leaders understand and support.

Get going!

Once senior management is aligned and on board, it's time to remediate risks. Many advances will be made behind the scenes, so those managing the process should frequently check in on contributors and stakeholders, keeping everyone in sync about expectations and timelines. Communication is vital—delays and surprises should be expected and managed, not hidden.

As noted, the most effective security depends on multiple layers of protection, starting with preventing compromise. We'll delve deeper into that topic in our next whitepaper.

ABOUT LODESTONE

Lodestone, a leader in comprehensive cyber defense, we're known for doing it differently. By blending best-in-class design, intelligent service and technology with human insight, our experts, provide clients with the information and processes needed to address cyber threats across the spectrum—from strategic readiness through digital forensics and incident response.

For more information on Lodestone, visit: Lodestone.com or contact us at info@lodestone.com

www.lodestone.com
320 E. Main Street
Lewisville, TX 75057