Resilience in the Time of **Ransomware** (I)

By **Isabel María Gomez,** Atento's **Global CISO**

ATENTO

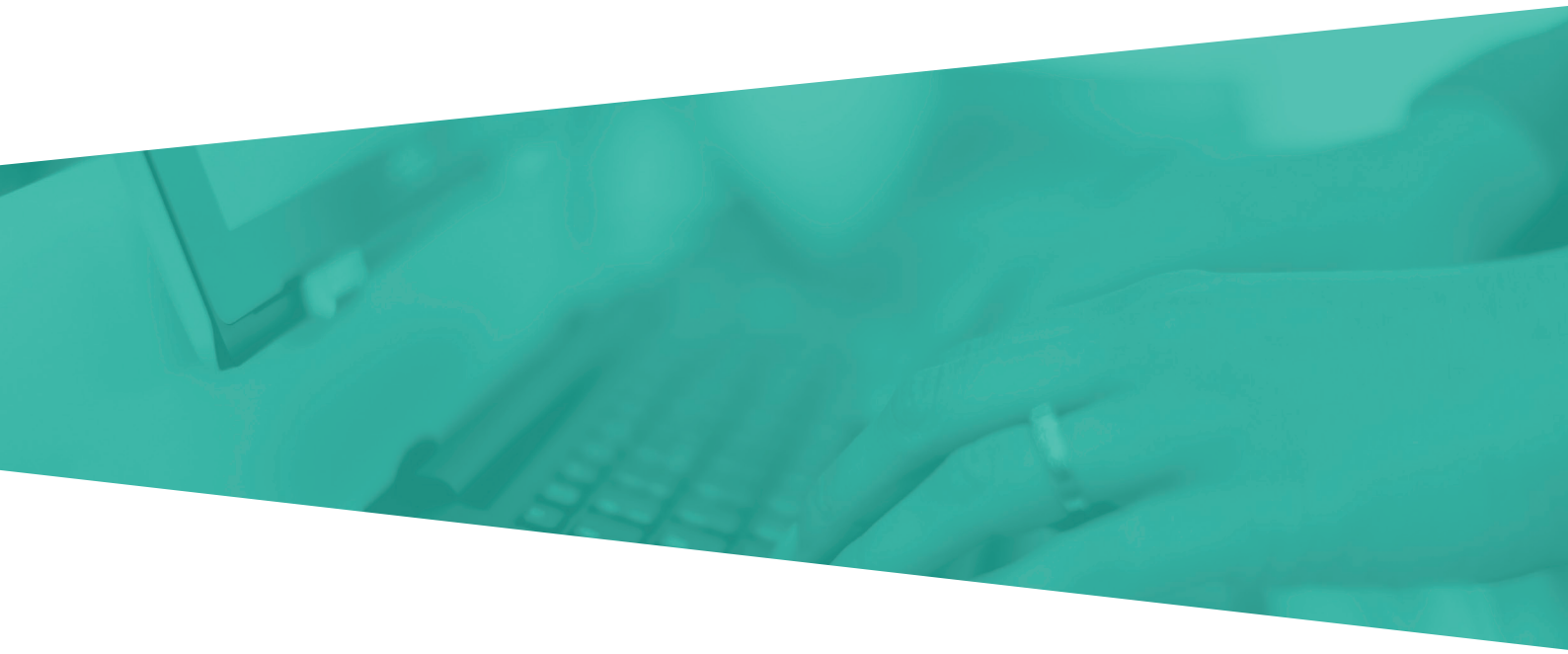
WHITE PAPER

CONTENT

01 Resilience in the Time of **Ransomware**

A ransomware attack is one of the most difficult scenarios facing companies today. It not only **puts the organization's business continuity processes to the test** but also creates a stressful scenario that goes beyond cybersecurity and technology, creating a need for action lines and decision-making processes that have rarely been tested so forcefully.

All the company's areas, without exception, become involved in an exercise that is no longer the boring, theoretical, controlled, and timed test in which everyone takes part to ensure recovery from a disaster scenario and which tends to be completed well before the expected deadline without any major setbacks, given its careful planning. **An actual ransomware attack is a real situation, which will test the true resilience of the security and technology leaders** responsible for providing support and leading the entire team's enormous efforts: ***There is no such thing as favorable wind if you do not know where you are heading.***



02 The moment **everything changes**

As in every disaster scenario, there is always a spark, a domino that falls and inexorably pushes over the other tiles around it: ***The start of a computer's encryption.*** The moment the **chief information security officer (CISO)** gets the call that activates the crisis committee is when the resilience of corporate cybersecurity is really activated. It is this person who must first make the right decisions that will contain and remedy the situation, while at the same time offering support and giving the best advice to the rest of the company to help prioritize each action line and put more wind in technology's sails: ***What is decided in those first moments will set the company's recovery time.***

By now, ransomware's attack method is common knowledge, although it cannot hurt to offer a brief reminder of the stages that occur when a cybercriminal gains access to your network, systems, and connected devices.

Ransomware attacks go through three stages that can be summarized as **three broad activities:**

- The cybercriminal breaks into your network, system, or devices;
- The cybercriminal takes control and deploys the ransomware; and
- The cybercriminal activates data encryption, destroys back-up copies, and steals the organization's and/or its customers' data, and then demands the payment of a ransom.

03 Origins

The malicious cybercriminal behind the threat tends **to find an entry point into your network** by:

- Launching brute-force attacks;
- Exploiting unresolved vulnerabilities; or
- Carrying out phishing attacks, in which the cybercriminal tries to request confidential information from an individual, group, or organization by mimicking or spoofing a particular, generally well-known brand to make a profit. The cybercriminal will try to trick the users into disclosing personal data, such as credit card numbers, online banking information, and other sensitive information, which will later be used to commit fraudulent acts.

04 Deployment

Once the cybercriminal has gained **entry to the network:**

- They will take control of your systems and connected devices, increasing their privileges if they had not done so already; and
- The malware will be deployed and infect your systems and connected devices with the ransomware.

05 Execution

Once they have gained **total control**, they will lower the defenses, possibly using global policies inside the forest or active directory, encrypt your data all at once, delete any available or connected back-up copies, and steal all possible data from the organization.

At this point, if they have succeeded in exfiltrating corporate data, it is possible that they will threaten to filter those data if the ransom is not paid, assuring you that your data will be unencrypted and your access to them restored if you pay up. This is something that they will undoubtedly do as it is the key to their business.

06 Some **technical tips** for improving resilience

Although the organizational elements will be explained in the second installment, it is important to note a series of **measures that any company can take** to help with early detection and to correlate alerts and information that make it difficult to execute this type of threat.

On this list of top cybersecurity measures against ransomware, it is advisable to stand back and, while keeping to what is already established and widely known, focus on a simple, feasible way to raise your level of resilience and protection against ransomware, something that will help your CISO protect you, whatever your company size.

1. **Install a local administrator password solution (LAPS)** on all workstations

   a. A LAPS offers local account password administration for domain-joined computers. The passwords are stored in an active directory (AD) and are protected by an access-control list, so that only eligible users can read a password or request its reset.

2. **Deactivate the server message block (SMB) server** on all domain workstations

   a. SMB is a client/server protocol that governs access to files, complete directories, and other network recourses, such as printers, routers, and interfaces open to the network.

   b. Link to recommended reading.

3. **Network segmentation**

   a. This is perhaps the top-ranking measure on this list, as its main goal is to reduce the attack surface area by applying rules that can lessen lateral movements risk and promote a zero-trust security policy, which only allows authorized traffic to go from a source to an authorized destination.

4. **Deactivate macros** in Word

   a. A macro is a series of commands and instructions that are grouped together under one command to complete a task automatically.

5. **Set up browser security policies** using a group policy object (GPO)

   a. Settings such as a phishing filter, password management, and certificate verification can protect an organization against web-based attacks when they are configured centrally and implemented on the organization's computers. This can be done using the GPO provided by Microsoft for Edge and Internet Explorer, and the ADMX templates for Chrome and Firefox made available by their respective browser providers.

6. **Local security authority subsystem service (LSASS) protection** against acquiring log-on details

a. LSASS is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens. It also writes to the Windows Security Log. *(Wikipedia)*

b. As lsass.exe is a crucial system file, its name is often faked by malware. The lsass.exe file used by Windows is located in the directory Windows\System32. If it is running from any other location, that lsass.exe is most likely a virus, spyware, trojan, or worm. Due to the way some systems display fonts, malicious developers may name the file something like lsass.exe (capital "i" instead of a lowercase "L") in efforts to trick users into installing or executing a malicious file instead of the trusted system file.)

c. Link to recommended reading.

7. **Create local firewall policies** by server role and activate them

a. After identifying the requirements and having information to hand on the design of the network and devices, you can start to design the rules and GPO settings that will allow you to apply these requirements to your devices.

b. Link to recommended reading.

8. **Implement Applocker** on all workstations

a. The AppLocker software lets you block certain applications, provided you have administrator permissions. This way you can decide which programs can run on the PC and prevent users from using applications you consider dangerous or inappropriate. This is a powerful function that allows you to increase your computer's security against external threats.

b. Link to recommended reading.

9. Migrate **unsupported operating systems**

a. It is often thought that it is better to deal with IT infrastructure as a whole, but this can lead to early obsolescence. In fact, hardware, software, and networks tend to be dealt with together. This common mistake means that the effects of obsolescence on each individual computer are not taken into account. Not all computers need the same types of programs and not all programs are used for the same type of work. It is advisable to analyze each computer separately in order to plan for the appearance of changes to its functionality.

10. Set up SMB signing and SMB3 for the entire company

a. SMB essentially signs each packet with a digital signature so that the client and server can confirm where they came from and the call's authenticity. When the SMB signature is activated, attackers are prevented from stealing SMB sessions, as they cannot alter the packets.

b. Link to recommended reading.

07 But it is not just a question of technology, there is **also due diligence**

If various technical measures have been applied and there is relative security and technological resilience, we now need to focus on another type of resilience that is also required to withstand an attack of this type: **due diligence.** Providing the company with an adequate cybersecurity framework is not enough: it will be the corporate values, and the people at the company's values, that will encourage the team to put in the enormous, exhausting effort required to bring the corporate ship into harbor quickly.

Among the ideas that will be developed in the second installment are adaptability, organizational response, and the legal and business impacts, including controlling information regarding the incident.

ATENTO

www.atento.com