REDUCING IMPACT OF RANSOMWARE ATTACKS VIA CLOUD-BASED APPROACHES

March 2019

Derek E. Brink, CISSP
Vice President and Research Fellow, Information Security and IT GRC

Ransomware is a top of mind threat for industries of all sizes, and is constantly being evolved and adapted by technically sophisticated and financially motivated attackers. To illustrate the importance of this issue in business terms, Aberdeen's simple analysis quantifies how the faster, more scalable time-to-recover provided by a **cloud-based backup and restore** capability reduces the impact of ransomware by about 90%.

Breaking Down the Relentless Risk of Ransomware

Although **ransomware** has been a weapon in the cybercriminal's arsenal since as early as 1989, it has more recently become a **top of mind threat for organizations of all sizes** in the wake of publicity that followed massive, worldwide ransomware attacks such as *Petya* (2016), *WannaCry* (2017), and *NotPetya* (2017).

Ransomware refers to malicious code designed to gain unauthorized access to data, and *encrypt* the data to block access by legitimate users. Attackers then demand that victims pay a ransom, in exchange for the key to decrypt and recover their own data.

Today, technically sophisticated and financially motivated attackers are constantly evolving and adapting their deployment of ransomware — to evade the protection mechanisms put in place by the defenders, and to maximize their own return on investment. Technical trends currently include high growth in **new ransomware variants**, as well as increased targeting of **mobile devices**, **connected devices** (i.e., IoT), **servers**, and **cloud-based services** in addition to **traditional enterprise endpoints**.

While the technical details and trends of ransomware are interesting and valuable for subject-matter experts, what enterprises ultimately need to understand is the **risk**. We often confuse technical information about *threats*, *vulnerabilities*, *exploits*, and *information technologies* with risk, and commonly use these terms interchangeably — but they are *not* synonymous with *risk*. This kind of technical information is about the "who," "what," and "how" of ransomware. Risk, on the other hand, is about the all-important "so what."

Risk, as properly defined, is always about "**how likely** is a successful ransomware attack to occur" for our organization, and "**how much** is the corresponding **business impact**." If we're not talking about *how likely* and *how much business impact*, we're not really talking about *risk*.

Breaking Down the Risk of Ransomware: How Likely?

From a variety of public sources, we can get a sense of several key factors for the *likelihood* side of the risk of ransomware:

- *More than half* of enterprises report that they've experienced **at least one ransomware attack** during the previous 12 months.
- Of those who were attacked, *most* are **attacked more than once**.
- *Most* ransomware attacks impact **traditional enterprise endpoints** — although increasingly they are also impacting the data on **mobile devices**, **connected devices** (i.e., IoT), on-premises **servers**, and **cloud-based services**.
- *About two-thirds* of ransomware attacks are successful in **infecting at least one endpoint**.
- *More than half* of successful ransomware attacks subsequently expand to **infect more than one endpoint**.
- Few organizations pay the ransom to recover their data — *almost all* can **restore from backups**.

The Traditional C.I.A. Triad of Information Security:

Confidentiality (or **privacy**) refers to data being accessible only to authorized users or systems.

Integrity refers to data being unaltered, except for intentional changes by authorized users or systems.

Availability refers to data being accessible when needed to authorized users or systems.

To date, the business impact of ransomware attacks has been related primarily to *availability*.

Breaking Down the Risk of Ransomware: How Much Impact?

Similarly, the *business impact* side of ransomware has several potential factors, including:

- **Lost productivity of users and responders** — i.e., the extent to which users are unable to do their jobs during the time their data is encrypted and unavailable. To date, such non-availability has been the primary business impact of ransomware.
- **Loss or exposure of sensitive data** — i.e., the extent to which ransomware results in a *data breach*, with its associated costs, fines, and / or penalties. To date, attackers have generally *not* been exfiltrating the encrypted data, just holding it for ransom and more immediate financial gain.
- **Loss of current revenue** — i.e., the extent to which data being encrypted and unavailable disrupts the generation of revenue during the time of disruption.
- **Loss of future profitability** — i.e., the extent to which the organization's handling of the ransomware attack results in lower

revenue (e.g., customers take their business elsewhere) or higher costs (e.g., higher marketing expenditures required to attract and retain new customers).

Key factors in *quantifying* the annualized business impact of ransomware attacks also include the **number of devices and users** who may be affected, the total **volume of data** to be recovered, and the **total time-to-recover**.

Quantifying the Risk of Ransomware: A Simple Case-in-Point, Focused on Traditional Enterprise Endpoints

To help the organization's senior leadership team **make a better-informed business decision** about the risk of ransomware, and what to do about it — *accept* it? *transfer* some of it to a third party? invest in additional capabilities to *manage* it to an acceptable level? — security professionals need to communicate about this issue more effectively, in the language of risk that the senior leaders already know and understand.

Technical details, scare tactics involving the latest headlines, standalone statistics, qualitative descriptions (e.g., "red / yellow / green"), or pseudo-quantitative assessments (e.g., "72 on a scale of 0 to 100") just aren't effective for this purpose. On the contrary, these approaches leave the business decisions to be made as they always have: on the intuition and judgment calls of the senior leadership team.

To illustrate how the risk of ransomware can be *quantified*, Aberdeen has developed a **Monte Carlo analysis** for a specific case-in-point: ransomware that impacts traditional **enterprise endpoints**.

For simplicity, Aberdeen's analysis:

- Focuses on **traditional enterprise endpoints**, which are still the most widely affected by ransomware attacks. (As previously noted, technical trends currently include increased targeting of **mobile devices**, **connected devices**, **on-premises servers**, and **cloud-based services** in addition to traditional enterprise endpoints. To be clear, *all* enterprise data should be backed up, available, and recoverable, regardless of the source.)
- Is based on a context of *1,000 enterprise employees* — with an assumption of one traditional enterprise endpoint per employee — and a total of *10 TB* of traditional endpoint data that potentially needs to be recovered.

In a **Monte Carlo analysis**, each variable in a calculation is expressed as a **range** (*lower bound*, *upper bound*) and a **shape** (*probability distribution*) — as opposed to as a static, single-point estimate.

The relevant calculations are then carried out based on a randomly selected value from the probability distribution for each variable, over many (say, 10,000) independent iterations.

In doing so, the result is also expressed as a range and distribution — as opposed to a misleading, static value such as "the average cost of a data breach is $201 per record."

Most importantly, the result can readily be represented in terms of both *how likely* and *how much business impact* — i.e., in terms of **risk**, as risk is properly defined.

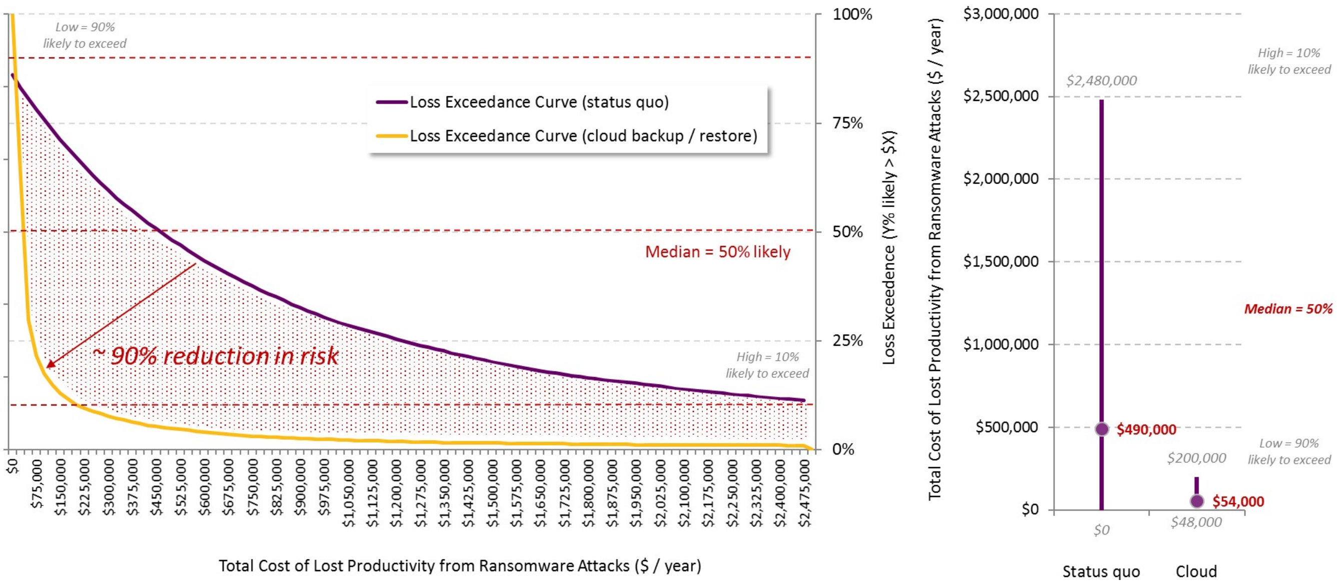
- Focuses on **lost productivity** as the primary business impact of ransomware, i.e., it does not consider the potential business impact of **data breaches**, **loss of current revenue**, or **loss of future profitability** as discussed above. This analysis therefore reflects a *conservative*, *understated* estimate of the total business impact of ransomware — factors which could be added, if necessary, to make a well-informed business decision about risk.

By estimating reasonable **ranges** (*lower bound*, *upper bound*) and **shapes** (*probability distribution*s) — based on the best available data — for the key factors of “how likely” and “how much impact” discussed above, Aberdeen’s simple Monte Carlo analysis quantifies the total cost of lost productivity as a result of ransomware attacks under the status quo backup and restore capabilities (see the **purple** line in Figure 1):

- The **median** annual cost of ransomware for an organization of 1,000 employees and 10 TB of data to backup and recover is about **$490K** …
- … with a **10% likelihood** that it will be **more than $2.5M**. The latter figure is an example of the “long tail” typical of security-related risks that’s so important for the senior leadership team to understand, to make a well-informed business decision regarding whether this level of risk is acceptable.

The risk of ransomware attacks impacts more than traditional enterprise endpoints — it puts larger sets of data that are critical to business operations via connected devices (i.e., IoT), on- premises servers, and cloud-based services. *All* enterprise data should be backed up, available, and recoverable, regardless of the source.

Figure 1: Quantifying How Cloud Backup / Restore Reduces the Risk of Ransomware, for Traditional Enterprise Endpoints



Source: Monte Carlo analysis for 1K endpoints, 10 Tb data; Aberdeen, March 2019

Options for reducing the risk of ransomware can include **reducing the likelihood** of successful ransomware attacks, e.g., by making incremental investments to improve:

- The *technologies* used for protection
- Operational *processes*, such as those used for patching vulnerabilities that are being exploited by ransomware
- *User* awareness and behaviors, to decrease the success of phishing attacks and malicious links as a delivery mechanism for ransomware

In addition, options for reducing the risk of ransomware can include **reducing the business impact** of successful ransomware attacks, e.g., by making incremental investments to improve the *recovery process*:

- Ransomware attacks will continue to adapt, evolve, and be successful — so *all* enterprise data should be backed up, available, and recoverable, regardless of the source.
- Successful ransomware attacks may affect not just a single user, but potentially the data on hundreds of devices — so backup and recovery solutions should enable data to be recovered device by device, or on an enterprise-wide scale.

Quantifying the Risk of Ransomware for Enterprise Endpoints, After Deployment of a Cloud-Based Backup / Restore Solution

For the "after" scenario, Aberdeen's analysis is based on the adoption of a **cloud-based backup and restore** capability, to reduce the business impact of a successful ransomware attack affecting enterprise endpoints:

- **Cloud-based backup and restore** solutions can provide *significantly faster time-to-recover* enterprise data, from a wide range of sources. For this scenario, **total time-to-recover** is based on empirical performance data made available to Aberdeen by a specific solution provider (*Druva inSync*).
- **Cloud-based backup and restore** solutions also provide a degree of isolation from an on-premises ransomware attack — e.g., in which a single enterprise endpoint is effectively "ground zero," from which the ransomware attack extends to impact many other devices, on-premises servers, and cloud-based services.

Quantifying How a Cloud-Based Backup / Restore Solution Reduces the Risk of Ransomware

Status quo:

- Median: $490K
- 10% likely: >$2.5M

After adopting a cloud-based backup / restore solution:

- Median: $54K
- 10% likely: >$200K
- ~90% reduction in the business impact of ransomware for traditional enterprise endpoints, net of the incremental investment
- ~90% likelihood that the reduction in business impact will exceed the cost of investing in a cloud-based backup and restore solution

- Finally, the business impact for the “after” scenario must also include an estimate for the **total annual cost of the solution** — because the benefits of faster time-to-recover don’t come for free.

After the deployment of a cloud-based backup and restore solution:

- The **median** annual business impact of ransomware in this scenario is reduced to about **$54K** …
- … with a **10% likelihood** that it will be **more than $200K**.

Said another way: The *faster, more scalable time-to-recover* provided by using a cloud-based backup and restore solution helps to reduce the risk of ransomware for enterprise endpoints by **about 90%** compared to the status quo, net of the incremental investment (see the orange line in Figure 1).

Aberdeen’s analysis shows that the *faster, more scalable time-to-recover* provided by using a cloud-based backup and restore solution helps to reduce the impact of ransomware by about 90% compared to current approaches.

Summary and Key Takeaways

- **Ransomware** is a top of mind threat for industries of all sizes, and is constantly being evolved and adapted by technically sophisticated and financially motivated attackers.
- To help the organization’s senior leadership team **make a better-informed business decision about the risk of ransomware** – and what to do about it – security professionals need to communicate about this issue more effectively, in the language of risk that the senior leaders already know and understand: *how likely*, and *how much business impact*?
- To illustrate the importance of this issue in business terms, Aberdeen’s simple analysis quantifies the risk of ransomware for **traditional enterprise endpoints** using current approaches:
    - For an organization of 1,000 users and 10 TB of data that potentially needs to be recovered, the **median** annual business impact of ransomware is **about $480K**, with **a 10% likelihood** of being **more than $2.5M**.
- After deployment of a **cloud-based backup and restore solution**:
    - The **median** annual business impact of ransomware in this scenario is reduced to **about $54K**, with **a 10% likelihood** of being **more than $200K**.

    - The *faster, more scalable time-to-recover* provided by deploying a cloud-based backup and restore solution helps to reduce the risk of ransomware for enterprise endpoints by **more than 90%**, net of the incremental investment.

- Enterprises considering a cloud-based backup and restore solution can significantly reduce the risk of ransomware attacks — not only for their **traditional enterprise endpoints**, but also for their **mobile devices**, **connected devices** (i.e., IoT), **on-premises servers**, and **cloud-based services**. *All* enterprise data should be backed up, available, and recoverable, regardless of the source.

Related Research

Quantifying How Disaster Recovery in the Cloud Reduces Your Risk: It's About Time; December 2018

Quantifying How Disaster Recovery as a Service Reduces Your Risk from Disruptions; August 2018

Enterprise Data in 2018: The State of Privacy and Security Compliance; March 2018

It's About Time: How Faster Database Recovery Reduces Risk; November 2017

About Aberdeen Group

Since 1988, Aberdeen Group has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen Group is headquartered in Waltham, Massachusetts, USA.

XXXXX