White Paper

Shielding Backup Data's Highly Exploitable Achilles Heel

With Infinidat InfiniGuard® and InfiniSafe®

by, Marc Staimer

2022

Research Premise

Ransomware has become the biggest threat to every IT organization regardless of its size. It represents more than 60% of the recoveries per a Dragon Slayer Consulting survey of 300+ Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS) managed service providers (MSP). And that number is an increase from 50% just a year earlier. It is reasonable to recognize that when MSPs are seeing a rapid rise in ransomware attacks in their customer base, it's also happening to their non-customers.

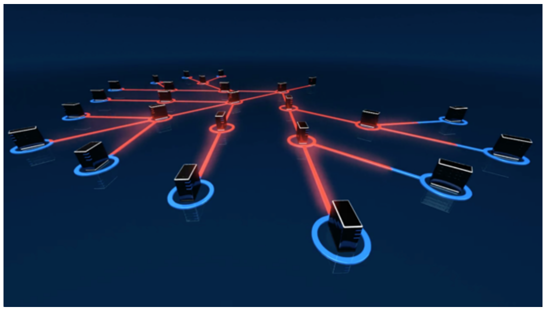
Ongoing market research validates this premise. Those statistics are provided in Appendix A.

Ransomware attacks radically raise anxiety levels in the most upbeat CIO. Ransomware has been evolving to evade the most common backend defenses such as a good sound backup, immutable storage, and immutable snapshots. That's a big problem. It's near impossible to recover from a ransomware attack without paying the ransom if there are no known good backups. Not good.

Cybersecurity professionals consistently recommend a multi-layered approach to cyber defense. These recommendations generally focus on the front door and include firewalls, anti-malware scanners at end points and servers, deep packet inspection, internal data behavioral heuristics, VPNs, extensive employee training, and a known good recent data backup.

The cyber criminals are not stupid. They know this. That's why they circumvent the front door by exploiting human weaknesses with targeted phishing. A simulated phishing campaign by the software security firm F-Secure[1] revealed why these attacks remain pervasive. More than 1/5th of the recipients of the simulated phishing emails purportedly from their human resources, clicked on the link. Amazingly, the technical staff were more likely to do so. That's how most ransomware gets past the front door.

[1] Dark Reading phishing analysis



Once the first machine is infected, they utilize tools to hide from virus scanners, then spread their infection utilizing the stolen privileges of the infected machine. Then rinses and repeats for each infected machine. Note that infection is not the same thing as detonation. A detonation occurs when the ransomware begins the encryption process.

Once the infection has spread as far as it can, the latest ransomware evolutions initiate a seek out and destroy mission to destroy or corrupt the backups. This has led to a new defense layer in the backend storage where the backup data is stored. It is commonly called immutable storage. Immutable storage means the data stored on a volume, file store, or object bucket is not changeable or deletable for a set period of time referred to as the retention period. That’s become a table stakes ransomware defense layer.

However, the cyber crooks have figured out a workaround. Just as they utilized targeted phishing to infect the organization, the also use similar sophisticated techniques to compromise the backup and storage admins credentials and privileges. This enables them to change the retention period of the backups. For example, instead of a three-month retentions period, they change it to three hours. Long enough for the admins to be satisfied that the backups, replicas, or snapshots are completed and verified and then poof...they’re gone, and no one notices. Then the ransomware detonates.

That’s not the only ransomware evolution. Remember that the latest versions infect, hide, and spread. They also are backed up, replicated, or snapped like the rest of data. That means they’re embedded in the backups, replicas, and snapshots. So even if they’re not deleted, they reinfect and detonate all over again as soon as they’re recovered. It becomes an attack-loop. Ransomware detonates. IT organization recovers from what it thinks is a good sound backup. Ransomware detonates again. Recovery again and repeat.

The IT organization has no idea when the last good backup occurred. They then have to make the calculation of how much data can they afford to lose – days, weeks, months? Or pay the ransom. Most will end up paying the ransom. That doesn’t mean they get 100% of their data back. It is quite common for the ransomware cyber criminal to not de-encrypt all of the sensitive or important data right away. They’ll ask for another ransom for the rest of the data. Keep in mind they are cyber criminals.

One more ransomware innovation is the double-extortion. The ransomware copies out sensitive data before it encrypts. The cyber criminals threaten to release the data if the ransom isn’t paid. Even if the ransom is paid, they’re cyber criminals. They frequently sell that data on the dark web to organizations that find it valuable.

What about cyber insurance? Cyber insurance rarely pays all of the ransom. The ransomware explosion in attacks and increase in ransom amounts has caused cyber insurance premiums to skyrocket. Insurance companies are in the business of making money, not losing it. They have become much pickier about who they’ll insure, what they cover, what defenses the insured must have in place, and the amount they’ll pay out.

All of this leads to the central premise: IT organizations must provide defense layers against all of these ransomware evolutions if they want to keep ransomware damage to a minimum. This is backup data’s highly exploitable Achilles heel. The question becomes how to shield it from ransomware exploitation?

Table of Contents

How to Shield Backup Data's Highly Exploitable Achilles Heel Problem

It starts by reverse engineering what the latest ransomware variants are designed to do and putting multiple roadblocks in their path. What cybersecurity experts recommend on the front door, must also be implemented for the backup data a.k.a. the back door. In other words, implement a multi-layered back door defense. Those defenses must protect against different attacks. Some of those defenses will be products, features, or services. Some of them are going to be processes and products.

Ransomware Layered Defense Requirements

The three ransomware attacks the backup storage must provide defenses for include the deletion, altering, or corruption of the backups, replicas, or snapshots; theft of storage admin privileges; and detection of embedded ransomware within the backups, replicas, or snapshots.

1. *Ransomware backup, replica, or snapshot destruction defense*

Ransomware actively seeks out and destroys backups. It will look for well-known backup repositories, replicas, and snapshots and either delete, alter, or corrupt them. Effective defenses require:

- Immutable storage or immutable snapshots. Immutability means data cannot be deleted or altered.
- Immutability tied to the retention policy. (It is both operationally and financially irresponsible to keep all backups forever. Backups are not archives and are costly substitutes with none of the advantages.)

2. *Ransomware storage admin privilege theft defense*

Ransomware actively targets the administrator with retention privileges to copy and steal those privileges. They then use those privileges to change the retention period to hours before automatic deletion making the backups disappear. Effective defenses require:

- Multi-factor authentication (MFA) for any action that affects the data or retention period. This is also known as deep MFA or stepped MFA.
- MFA must be on a separate device, preferably one that uses biometric recognition such as a fingerprint or facial recognition.

3. *Ransomware embedded within the backups, replicas, and snapshots defense*

Ransomware lies dormant for months getting backed up every day with the rest of the data. When the ransomware detonates, all recoveries will reinstall the same ransomware detonating over and over and over again. Effective defenses require a combination of product and process:

- Backups, replicas, or snapshots must be recovered on a weekly or more frequent basis, in a logical or physical air gapped environment.
- Work with the most common data protection software in the market.
- Accomplishing those recoveries frequently requires the storage to be extremely fast with very high throughput and near instantaneous recovery speeds to accelerate the process. Otherwise, it becomes too time consuming. A lengthy process will likely be done far less frequently making it less effective. This is especially true in large enterprise accounts. Data protection software commonly utilizes multiple physical or virtual machines to copy data out from production servers, endpoints, SaaS, databases, and more. The target storage must be able to handle multiple concurrent streams at a very high throughput. And it must be affordable and cost effective. There are plenty of primary storage systems with the throughput required. But excessive costs generally make it unattractive and unsustainable as a target for data protection software.
- Frequency to be determined by cyber resilience recovery point objective (RPO), which is the amount of data the organization can afford to lose.
- Recoveries must then be scanned by the most up-to-date signatureless anti-ransomware software.

- Every backup, replica, and snapshot that comes up clean should be noted as a good backup for recovery purposes.
- Any ransomware detected should immediately be identified and quarantined.
- Leverage that knowledge to immediately remove those same infections from the compromised production systems.

The Infinidat Solution – InfiniGuard® with InfiniSafe®

Infinidat highly modified its award-winning software defined InfiniBox storage system with three data deduplication engines (DDE) – one of the three is for redundancy in case there is a failure – and multi-layered cyber resilience to turn it into a purpose-built backup appliance (PBBA) specifically architected for data protection called InfiniGuard. It is tested, validated, and certified with all of the most popular data protection software suites such as Veeam, Commvault, Veritas, Oracle RMAN, IBM Spectrum Protect, NetWorker, and many more.

What makes InfiniGuard stand out is the built-in cyber resilience of InfiniSafe, which comes standard with all InfiniGuard systems, included at no additional charge. InfiniSafe meets each of the requirements previously described, for meeting the cyber resilience demands in a modern ransomware defense infrastructure. It provides multiple layers of defense against ransomware with:

1. Immutable snapshots tied to retention policies, capturing the comprehensive DDE engine backup information including all configurations, logs, and data. This protects all of the point-in-time (PIT) snapshots from modification, deletion, corruption, change in policy, or any other action.

   It also protects shares, folders, files, users, passwords, logs, network configs, and share access – an exclusive InfiniSafe capability. In addition, the highly efficient deduplication, and the space efficient WORM (write once, read many) technology, minimizes the capacity consumed, further reducing costs.

2. Deep multi-factor authentication (MFA) for any changes the admin attempts to make foiling ransomware's theft of privileges.

3. Recovery logical air-gapped/fenced protection to make sure backups can be scanned, tested, and validated without fear of ransomware escaping to other machines. All in a single highly resilient system. Most other PBBAs or backup target storage systems require a minimum of two systems at twice the cost to provide a logical air-gapped/fenced environment.

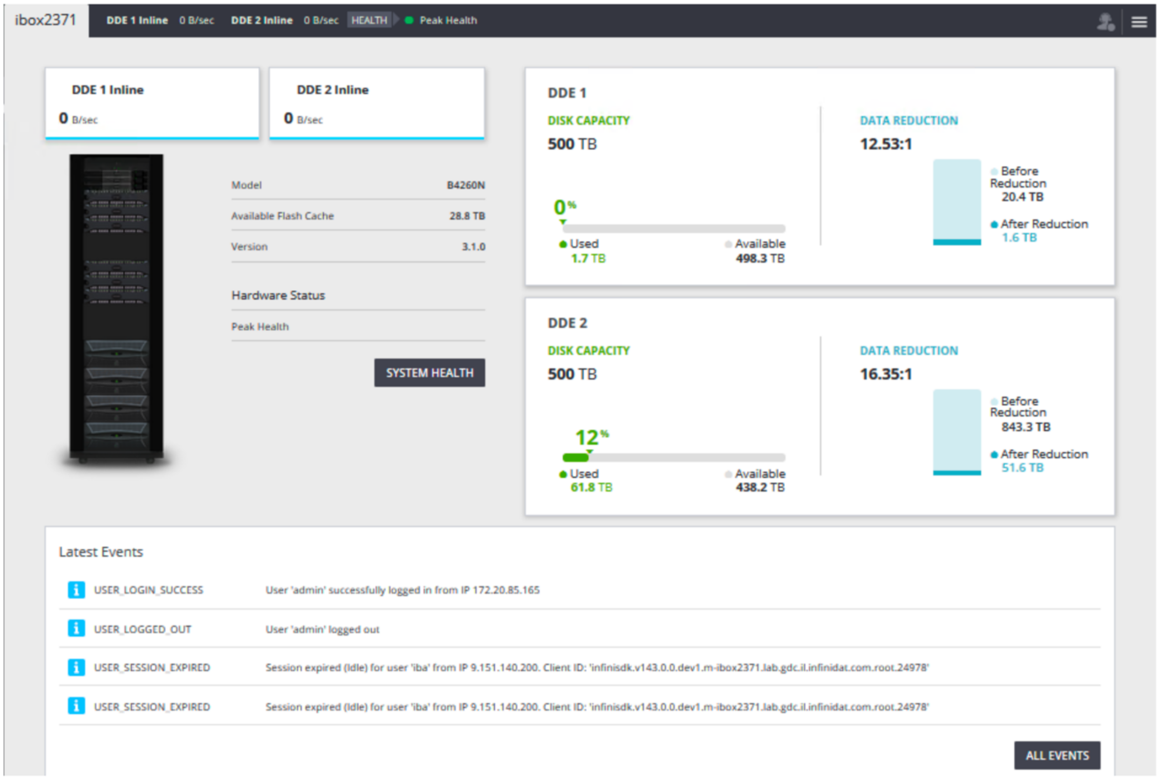
4. Best-in-class throughput performance with up to 180TB/hr with NetBoost[2] and three (one for redundancy and enhanced availability) integral deduplication engines within the system. That performance is an increase of 2x the previous InfiniGuard iteration. This halves the backup window that is so important for those full volume backups.

5. Near instantaneous recoveries at scale – not just MTree Files and Folders – to a validated recovery point, regardless of size. This can represent up to 25PB of protected data per DDE or up to 50PB per InfiniGuard. Near instantaneous recoveries is exceedingly important when recovering from a ransomware attack. Every second counts and time is not a friend. Downtime is extremely costly to every organization. Minimizing it is essential. The key is what is meant by instantaneous recoveries. Most data protection vendors mean 30 minutes or less. Infinidat is aiming at much less. They are able to demonstrate a 1.5 PB Veeam backup recovery in 12 minutes 15 seconds.

InfiniSafe's extensive cyber resilience is just part of what comes with InfiniGuard. InfiniGuard is built on the production proven technologies of InfiniBox and InfiniBox SSA. It comes with Infinidat's no compromise

[2] Source deduplication software from Infinidat.

performance, intuitive setup, management, operations, and control with an instinctively easy UI. And a very low total cost of ownership (TCO)[3]. Here is an example of that InfiniGuard Intuitive UI Dashboard.



DDE 1 Inline
0 B/sec

DDE 2 Inline
0 B/sec

Model B4260N
Available Flash Cache 28.8 TB
Version 3.1.0

Hardware Status
Peak Health

DDE 1
DISK CAPACITY
500 TB
0%
Used 1.7 TB
Available 498.3 TB
DATA REDUCTION
12.53:1
Before Reduction 20.4 TB
After Reduction 1.6 TB

DDE 2
DISK CAPACITY
500 TB
12%
Used 61.8 TB
Available 438.2 TB
DATA REDUCTION
16.35:1
Before Reduction 843.3 TB
After Reduction 51.6 TB

Latest Events

```
USER_LOGIN_SUCCESS      User 'admin' successfully logged in from IP 172.20.85.165
USER_LOGGED_OUT         User 'admin' logged out
USER_SESSION_EXPIRED    Session expired (Idle) for user 'iba' from IP 9.151.140.200. Client ID: 'infinisdk.v143.0.0.dev1.m-ibox2371.lab.gdc.il.infinidat.com.root.24978'
USER_SESSION_EXPIRED    Session expired (Idle) for user 'iba' from IP 9.151.140.200. Client ID: 'infinisdk.v143.0.0.dev1.m-ibox2371.lab.gdc.il.infinidat.com.root.24978'
```

The InfiniGuard Dashboard displays the following information about the system:

- Current throughput rate.
- Current I/O rate. Operational State
- InfiniGuard operational state. Except from the start-up of the system, the state should always be Active.
- InfiniGuard model.
- Amount of system flash cache.
- Software version that is installed on the system.
- Both visual and textual indicators on the state of the system's hardware components.
- Amount of used capacity out of available usable capacity.
- Rolling list of the latest system events.

None of that would matter if InfiniGuard were exceedingly difficult to use. It’s the opposite. Infinidat built in intuitive automation. Many of the manual tasks typical with PBBAs are gone. Immutable snapshots are automated with advanced “Set & Forget It” capability. There are no RAID groups to build or manage. Everything from the DDE engine failover to the immutable snapshots and logical air-gapping is a single click or “button”. In other words, InfiniGuard does not require extensive training, skill sets, or expertise to fully utilize.

[3] Infinidat does not charge any additional license fees for InfiniSafe. It is an integral part of InfiniGuard. Highly efficient deduplication with WORM reduces capacity requirements lowering TCO.

InfiniGuard has an exceptional record of availability and reliability. It's built to the Enterprise standard of complete system level redundancy. It protects data from end-to-end silent data corruption. It can optionally create a site-to-site replicas at a second InfiniGuard.

InfiniGuard is the best of both worlds for cyber resilience and disaster recovery.

Summary and Conclusion

Ransomware is the technology plague of the early 21st century. It has become a multi-billion-dollar business with profits poured back into research and development. Ransomware continues to evolve with new variants ongoing. The cyber criminals are relentless and remorseless. IT pros be as well. Failure to fight back effectively is fiduciary negligence.

There are no magic silver bullet products or services that can guarantee 100% protection from ransomware today and likely never will be. No shield is impenetrable. The key to protecting the organization's data is with a defense in-depth, a.k.a. layered defense. The goal is to make it more difficult and much harder for the cyber criminals to get ransom from the IT organizations with a layered defense than the ones without it. They will more often than not take the path of lesser resistance.

To deliver that layered defense today means making it difficult to impossible to delete, change, alter, or corrupt the backups, replicas, or snapshot. It also means defending against stealing admin privileges that allow them to circumvent immutable storage retention timeframes. Finally, it means defending against dormant ransomware infections embedded within backups, replicas, or snapshots from preventing recoveries.

Infinidat has delivered that in spades with the InfiniGuard PBBA and built-in InfiniSafe. It has the immutable snapshots combined with multi-factor authentication that stops the cyber criminals from be able to delete, change, alter, corrupt, or change the retention timeframes of those immutable snapshots. The logical air-gapping/fenced forensic network in combination with the near instantaneous recoveries enables snapshots to be mounted and scanned for ransomware, preventing embedded ransomware sabotage.

In today's highly aggressive ransomware environment, Infinidat's InfiniGuard with InfiniSafe solution is a very effective layered defense and shield against backup data's highly exploitable Achilles heel.

For More Information on InfiniGuard

Go to: Infinidat InfiniGuard and InfiniSafe

Paper sponsored by Infinidat. **About DSC:** Marc Staimer, as President and CDS of Dragon Slayer Consulting in Beaverton OR since 1998, is well renowned for his in-depth and keen understanding of user problems, especially with storage, networking, applications, cloud services, data protection, and virtualization. Marc has published thousands of technology articles and tips from the user perspective for internationally renowned online trades including many of TechTarget's Searchxxx.com websites, Wikibon, Network Computing, and GigaOM. Marc has additionally delivered hundreds of white papers, webinars, and seminars to many well-known industry giants such as: Brocade, Cisco, DELL, EMC, Emulex (Avago), HDS, HPE, LSI (Avago), Mellanox, NEC, NetApp, Oracle, QLogic, SanDisk, Toshiba, and Western Digital. He has additionally provided similar services to smaller, less well-known vendors/startups including: Asigra, BrainChip, Cloudtenna, Clustrix, Condusiv, DH2i, Diablo, FalconStor, Gridstore, ioFABRIC, Nexenta, Neuxpower, NetEx, NoviFlow, Pavilion Data, Permabit, Qumulo, SBDS, StorONE, Tegile, and many more. His speaking engagements are always well attended, often standing room only, because of the pragmatic, immediately useful information provided. Marc can be reached at marcstaimer@me.com, (503)-312-2167, in Beaverton OR, 97007.

Appendix A: Disturbing Varonis Accumulated Ransomware Statistics

General Ransomware Statistics

- Ransomware remains the most prominent malware threat. (Datto, 2019)
- Malicious emails are up 600% due to COVID-19. (ABC News, 2021)
- 37% of respondents' organizations were affected by ransomware attacks in the last year. (Sophos, 2021)
- In 2021, the largest ransomware payout was made by an insurance company at $40 million, setting a world record. (Business Insider, 2021)
- The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020. (National Security Institute, 2021)
- Experts estimate that a ransomware attack occurred every 11 secs in 2021. (Cybercrime Magazine, 2019)
- About 1 in 6,000 emails contain suspicious URLs, including ransomware. (Fortinet, 2020)
- The average downtime a company experiences after a ransomware attack is 21 days. (Coveware, 2021)
- 71% of those who are affected by ransomware have been infected. Half of the ransomware attacks that are successful infect at least 20 computers in the organization. (Acronis, 2020)
- The most common tactics hackers use to carry out ransomware attacks are email phishing campaigns, RDP vulnerabilities, and software vulnerabilities. (Cybersecurity & Infrastructure Security Agency, 2021)
- 65% of employers allow their employees to access company applications from unmanaged, personal devices. (Bitglass, 2020)
- From a survey conducted with 1,263 companies, 80% of victims who submitted a ransom payment experienced another attack soon after, and 46% got access to their data but most of it was corrupted. (Cybereason, 2021)
- Additionally, 60% of survey respondents experienced revenue loss and 53% stated their brands were damaged as a result. (Cybereason, 2021)
- 29% of respondents stated their companies were forced to remove jobs following a ransomware attack. (Cybereason, 2021)
- 42% of companies with cyber insurance policies in place indicated that insurance only covered a small part of damages resulting from a ransomware attack. (Cybereason, 2021)

Healthcare Specific

- Over 2,100 data breaches in the healthcare industry have been reported since 2009. (Tech Jury, 2021)
- Healthcare organizations dedicate only around 6% of their budget to cybersecurity measures. (Fierce Healthcare, 2020)
- Ransomware attacks were responsible for almost 50% of all healthcare data breaches in 2020. (Health and Human Services, 2021)
- Attacks on healthcare cost more than any other industry at $408 per record. (HIPAA Journal, 2020)
- Ransomware attacks against U.S. healthcare providers have caused over $157 million in losses since 2016. (HIPAA Journal, 2020)
- In 2020, 560 healthcare facilities were affected by ransomware attacks in 80 separate incidents. (Emsisoft, 2021)
- Nearly 80 million people were affected by the Anthem Breach in 2015, the largest healthcare data breach in history. (Wall Street Journal, 2015)
- Healthcare received 88%t of all ransomware attacks in the United States in 2016. (Becker's, 2016)
- In September 2020 alone, cybercriminals infiltrated and stole 9.7 million medical records. (HIPAA Journal, 2020)

Education Specific

- Ransomware attacks against universities increased by 100% between 2019 and 2020. (BlueVoyant, 2021)
- The average cost of a ransomware attack in the higher education industry is $447,000. (BlueVoyant, 2021)
- Since 2020, 1,681 higher education facilities have been affected by 84 ransomware attacks. (Emsisoft, 2021)
- 66% of universities lack basic email security configurations. (BlueVoyant, 2021)
- 38% of analyzed universities in the Cybersecurity in Higher Education Report had unsecured or open database ports. (BlueVoyant, 2021)
- Cyberattacks against K-12 schools rose 18% in 2020. (K-12 Cybersecurity, 2020)
- A school district in Massachusetts paid $10,000 in Bitcoin after a ransomware attack in April 2018. (Cyberscoop, 2018)

Finance & Insurance Specific

- 62% of all records leaked in 2019 were from financial institutions. (Bitglass, 2019)
- Over 204,000 people experienced a login attempt to access their banking information. (Hub Security, 2021)
- 90% of financial institutions have been targeted by ransomware attacks. (PR Distribution, 2018)
- There's a rising threat to small financial institutions with less than $35 million in revenue. (National Credit Union Administration, 2019)
- In 2020, 70% of the 52% of attacks that went after financial institutions came from the Kryptik Trojan malware. (Hub Security, 2021)
- LokiBot has targeted over 100 financial institutions, getting away with more than $2 million in revenue. (Hub Security, 2021)
- Banks experienced a 520% increase in phishing and ransomware attempts between March and June in 2020. (American Banker, 2020)

Government Specific

- In 2020, 33% of attacks on governmental bodies were ransomware (Security Intelligence, 2020)
- In June 2019, a city in Florida paid a $600,000 ransom to recover hacked files. (CBS News, 2019)
- Only around 38% of local and state government employees are trained in ransomware attack prevention. (IBM, 2020)
- A ransomware attack against a Southern city in 2020 cost over $7 million. (SC Magazine, 2020)
- A ransomware attack struck an East coast city in 2019 and caused a loss of over $18 million. (Baltimore Sun, 2019)
- In 2019, 226 U.S. city mayors in 40 states agreed to a pact that denies ransom payments to cybercriminals. (Hashed Out, 2020)
- In 2019, attacks against municipalities increased 60% from the year before. (Kaspersky Labs, 2019)
- The top cybersecurity story in 2019 was ransomware attacks against state and local governments. (Government Technology, 2019)
- 48 of the 50 U.S. states were affected by at least one ransomware attack from 2013 to 2018. (Bank Info Security, 2019)

Ransomware Costs

- The value of ransom demands has gone up, with some demands exceeding over $1 million. (Cybersecurity & Infrastructure Security Agency, 2021)
- The cost of ransomware attacks surpassed $7.5 billion in 2019. (Emsisoft, 2019)
- In 2021, the average payout by a mid-sized organization was $170,404. (Sophos, 2021)

- In May 2021, Chief Executive paid hackers $4.4 million in bitcoin after receiving a ransom note. (The Wall Street Journal, 2021)
- In Q1 2017, FedEx lost an estimated $300 million from the NotPetya ransomware attack. (Cyberscoop, 2021)
- The average cost to recover from a ransomware attack is $1.85 million. (Sophos, 2021)
- Damage as a result of ransomware attacks was over $5 billion in 2017 — 15 times the cost in 2015. (Cyber Security Ventures, 2017)
- Downtime costs are up 200% year-over-year (2019 vs. 2018). (Datto, 2019)
- On average, ransomware attacks cause 15 business days of downtime. Due to this inactivity, businesses lost around $8,500 an hour. (Health IT Security, 2020)
- Ransomware that attacked an unnamed oil and gas company cost $30 million. (Datto, 2017)
- The hacker group behind an oil company attack allegedly acquired $90 million in ransom payments in only nine months from around 47 victims. (Fox Business, 2021)
- Four times as many businesses affected by ransomware attacks with over 100 employees reported paying ransoms. (Dark Reading survey, 2020)

Ransomware Projections and Future Trends

- The total ransomware costs are projected to exceed $20 billion in 2021. (Cybercrime Magazine, 2019)
- Cybersecurity Ventures predicts that ransomware will cost $6 trillion annually. (Cybersecurity Ventures, 2020)
- In the future, there will be an increase in organizations that will switch to zero-trust security models due to the vulnerability of identity-based threats. (RSA Security, 2020)
- Remote workers will be the main target of cybercriminals throughout 2021. (Security Magazine, 2020)
- 84% of organizations will keep remote work as the norm even after COVID-19 restrictions are lifted, resulting in an increase of internet users and a greater risk of data exposure. (Bitglass, 2020)
- Future hackers will target stay-at-home workers since personal devices are easier to hack than office hardware. (Security Magazine, 2020)