BITSIGHT

EBOOK

Ransomware: The Rapidly Evolving Trend

Ransomware: The rapidly evolving trend

Ransomware continues to be one of the most significant cyber threats worldwide, regardless of a company's size or industry. One in four breaches involve ransomware, and it appears in more than 62 percent of all incidents committed by organized crime actors[1]. The threat of ransomware is compounded by a distributed workforce, trends toward technology consolidation, geopolitical upheaval, and budget constraints. Cyber criminals are taking advantage of these new opportunities to exploit a greatly expanded attack surface.

Ransomware attacks doubled in 2021[2], then spiked again in the first half of 2022[3].

The overall cost of recovering from a ransomware incident is trending upwards[1].

On average, businesses experience 20 days of downtime from ransomware[4].

One in four consumers will abandon a product or service after a ransomware-related disruption[5].

From May 2021–June 2022, ransomware groups took credit for 3,640 incidents on their webpages[6].

While ransomware itself isn't new, it's growing more and more sophisticated. With such a great potential to earn money, Ransomware-as-a-Service (RaaS) groups have grown more organized, such as leveraging traditional business models. For example, internal chat logs from Conti RaaS group leaked in February 2022 showing that the group included middle management, HR managers, technical teams, and employee benefits[9].

But cyber attacks don't "just happen." Cyber criminals take advantage of vulnerabilities, stolen credentials, phishing, malicious code on web pages, and social engineering to steal a company's information and sell it back to them. Ransomware group Maze emerged in late 2019, operating a "double extortion" strategy[7]. And the first case of triple extortion appeared in October 2020[8]. In the chart on the following page, you can see some of the tactics and targets of ransomware attacks. But, organizations can defend against the risk of ransomware with the right data and industry-leading cybersecurity technology.

Extortion Type	Definition	Example
Single	Attackers demand a ransom for: 1) the decryption key	Attackers stole Colonial Pipeline's data, providing the decryption key upon payment.
Double	Attackers demand a ransom for: 1) the decryption key 2) not publishing exfiltrated data on the dark web to the impacted organization	Ransomware operators targeted Westech International's data, threatening to sell compromised data on the dark web.
Triple	Attackers demand a ransom for: 1) the decryption key 2) not publishing exfiltrated data on the dark web to the impacted organization 3) not publishing exfiltrated data on the dark web to the impacted individual	Cybercriminals extorted Finnish psychotherapy clinic Vastaamo to regain access to its files and to avoid having sensitive patient records published, and then extorted the patients to prevent their individual records from being published.

What Bitsight has learned—and how we can help

While no organization is immune from facing determined cyber criminals, there are best practices for minimizing the likelihood of experiencing a successful ransomware attack. Chief among them is a relentless focus on cyber hygiene—with the goal of ensuring that security controls, practices, and team members are performing effectively every day. Good cyber hygiene significantly lowers the chance of cyber incidents.

At its core, cyber hygiene is a set of essential practices and tasks a company uses to keep systems, data, and users secure. There are a multitude of practices that a company should implement to improve cyber hygiene, but some are more statistically correlated to the likelihood of experiencing a cyber incident. Over the course of two and a half years, Bitsight's research team analyzed hundreds of ransomware events to estimate the relative probability that an organization will experience a ransomware event. The analysis looked back over five six-month periods benchmarked against companies with a high Bitsight Security Rating for security effectiveness.

In particular, Bitsight identified greater risk based on four key areas:

- **The Bitsight Security Rating (Rating).** Organizations with a lower Rating increasingly become more likely to become a ransomware target.
- **Patching cadence.** Poor patching performance correlates to a nearly sevenfold increase in ransomware risk for companies with a C grade or lower.
- **TLS/SSL Configurations.** Companies with a C grade or lower in TLS/SSL Configurations are nearly four times more likely to be a ransomware target.
- **TLS/SSL Certificates.** Companies with a C grade or lower in TLS/SSL Certificates are roughly three times more at risk of a ransomware incident.

Risk based on Bitsight Rating

Organizations with a Rating lower than 600 are 6.4 times more likely to be a ransomware target—and organizations with a Rating between 600-650 are 4.6 times more likely—compared to the benchmark of organizations with a 750 and over Rating. Bitsight continuously and nonintrusively assesses organizational cybersecurity performance by evaluating security performance observations across 23 different categories, including compromised and exposed systems, critical vulnerabilities, patching cadence, software security, and other key issues. **Figure 1** shows the increase in ransomware risk compared to a lower Rating.

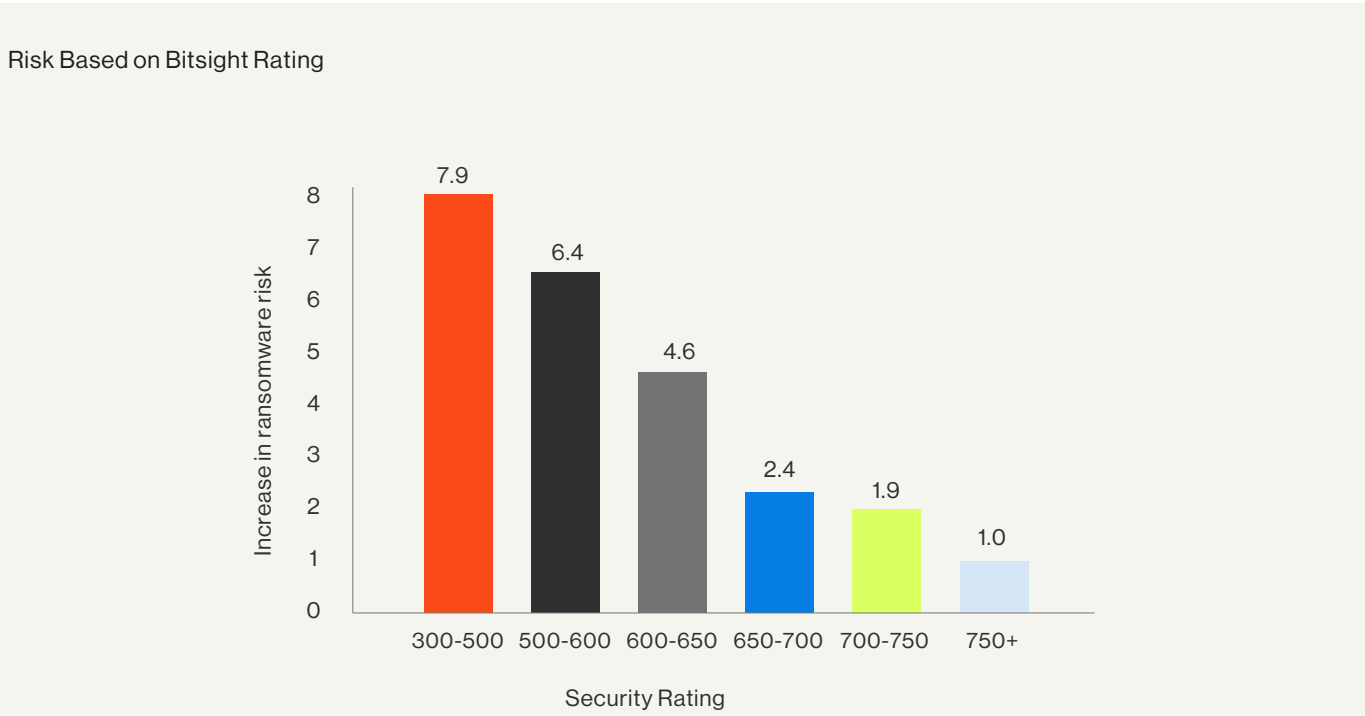

Figure 1: Increased likelihood of ransomware risk relative to organizations with a 750 and over Bitsight Rating as measured by Bitsight.

Risk based on patching cadence grade

Patching cadence is the elapsed time between software between when software patches become available compared to when those patches are implemented. Generally, patches resolve gaps affected by important vulnerabilities, or publicly disclosed weaknesses that an attacker could use to gain unauthorized access. Poor patching performance correlates to a nearly sevenfold increase in ransomware risk for companies with a C grade or lower. **Figure 2** shows the increase in ransomware risk compared to a lower letter grade.

Letter grades provide a quick way to understand how a company is performing in each risk type, as well as a meaningful way to compare risk type performance of one company to another. They are directly correlated to how well a company is performing, relative to all companies in the Bitsight inventory. Below is a table that outlines how each grade correlates to their performance, relative to their company size:

Grade	Percentile
A	In the top 10% of companies
B	In the top 30% of companies
C	In the top 60% of companies
D	In the bottom 40% of companies
F	In the bottom 20% of companies

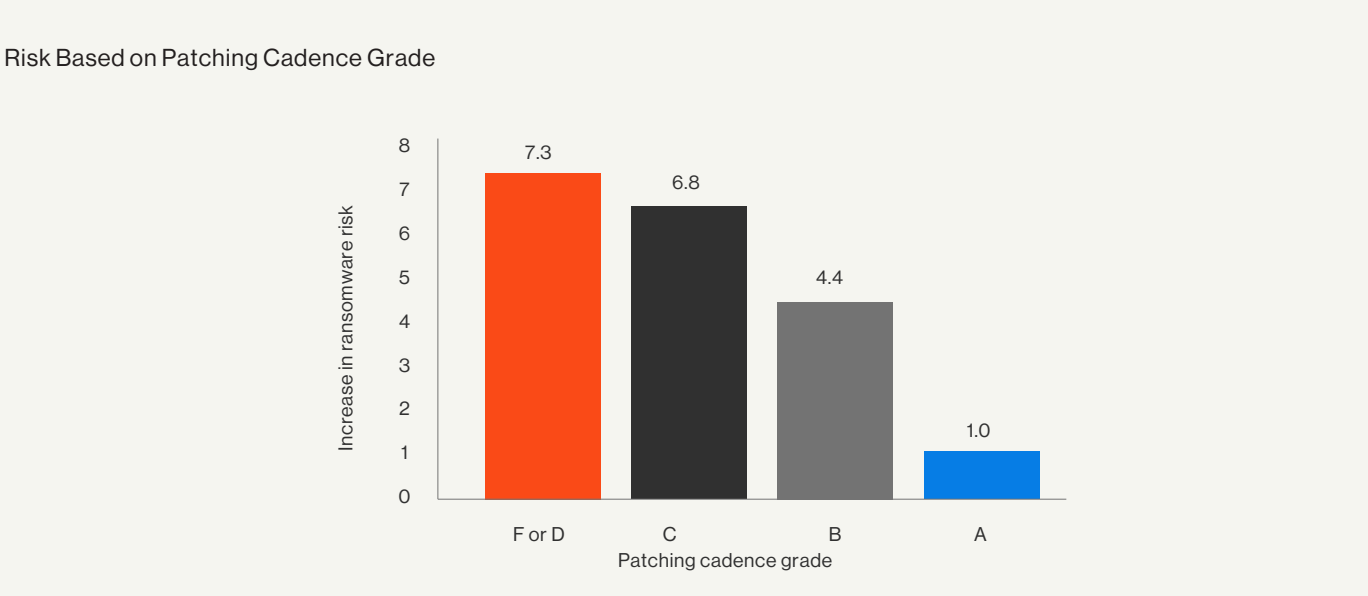

Figure 2: Increased likelihood of ransomware risk relative to organizations with a 750 and over Bitsight Rating in regards to Patching Cadence letter grade as measured by Bitsight.

Risk based on TLS/SSL Certificate and Configurations Grades

TLS/SSL certificates and configurations are the encryption protocols and certificates that a security team uses to ensure the connections between a user, a website, and a machine are encrypted and secure. Companies with a C grade or lower in TLS/SSL Configurations are nearly four times more likely to be a ransomware target, and companies with a C grade or lower in TLS/SSL Certificates are roughly three times more at risk of a ransomware incident, as shown in **Figure 3**.

It's unlikely that lapsed TLS/SSL encryptions would be the direct cause of a ransomware attack. But, it indicates that the cybersecurity program has poor cyber hygiene and may have gaps in vulnerability management, a challenge with Shadow IT, or program management, all of which increases cyber risk. For example, if a TLS or SSL certificate expires on a company's website, then any visitor will receive a warning message or may not even be able to access it at all. This is a common symptom of a copy-cat website, which may impact the trust that a visitor has in the company's brand, or make it easier for an attacker to spoof the website. An expired configuration may potentially expose critical information.

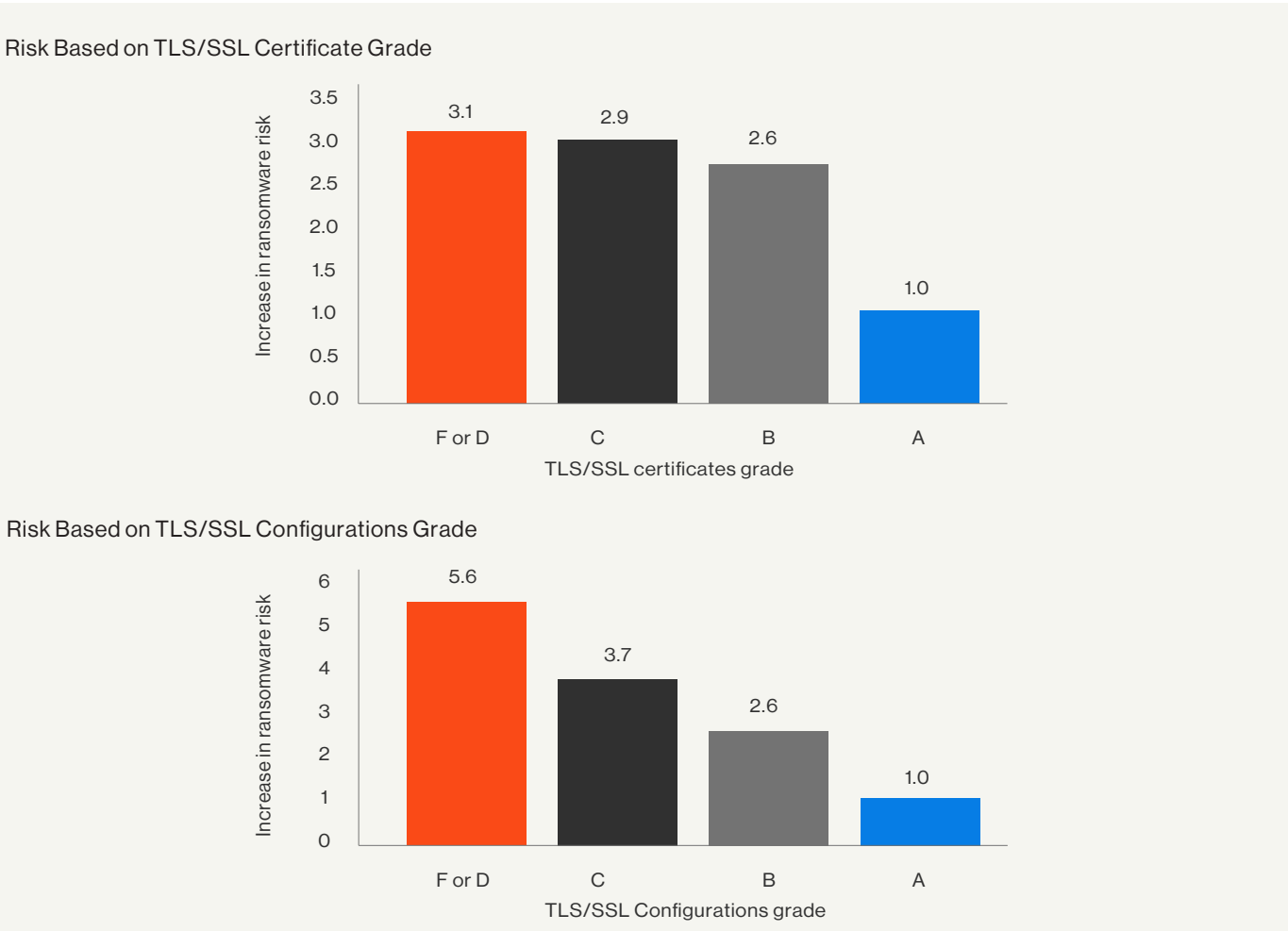

Figure 3: Increased likelihood of ransomware risk relative to organizations with a 750 and over Bitsight Rating in regards to TLS/SSL Certificate & Configurations letter grade as measured by Bitsight.

Cyber hygiene matters

The research demonstrates the correlation of Bitsight's performance in four analytics, including the Rating and three risk vector grades, that provide clear ransomware risk indicators. While each of these four areas on their own may not be a direct cause of ransomware, a poor score in any of these areas suggests poor cyber hygiene in multiple areas of a cybersecurity program. While the Rating and risk vectors offer specific evidence, the reducing ransomware risk will come from an overall improvement in cyber practices.

Companies that demonstrate strong cyber health have a lower risk of successful ransomware and other cyber attacks, offering a variety of positive benefits:

- Preventing catastrophic outcomes, such as financial losses and business downtime
- Instilling stronger brand reputation and trust with partners, vendors, and customers
- Increasing the chance of gaining cyber insurance coverage and better premiums

REFERENCES

[1] https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

[2] https://pages.checkpoint.com/cyber-attack-2021-trends.html

[3] https://www.helpnetsecurity.com/2022/08/12/increase-ransomware-attacks/

[4] https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/

[5] https://www.arcserve.com/blog/consumers-sound-impact-ransomware-purchasing-behavior-and-brand-loyalty

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

[7] https://www.itpro.com/security/ransomware/367624/the-rise-of-double-extortion-ransomware

[8] https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

[9] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Interested in seeing how effective you are at preventing the risk of ransomware?
Get your organization's Bitsight Security Rating and see how your security compares to industry benchmarks.

Get the report →

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT