BITSIGHT
The Standard in SECURITY RATINGS

EBOOK

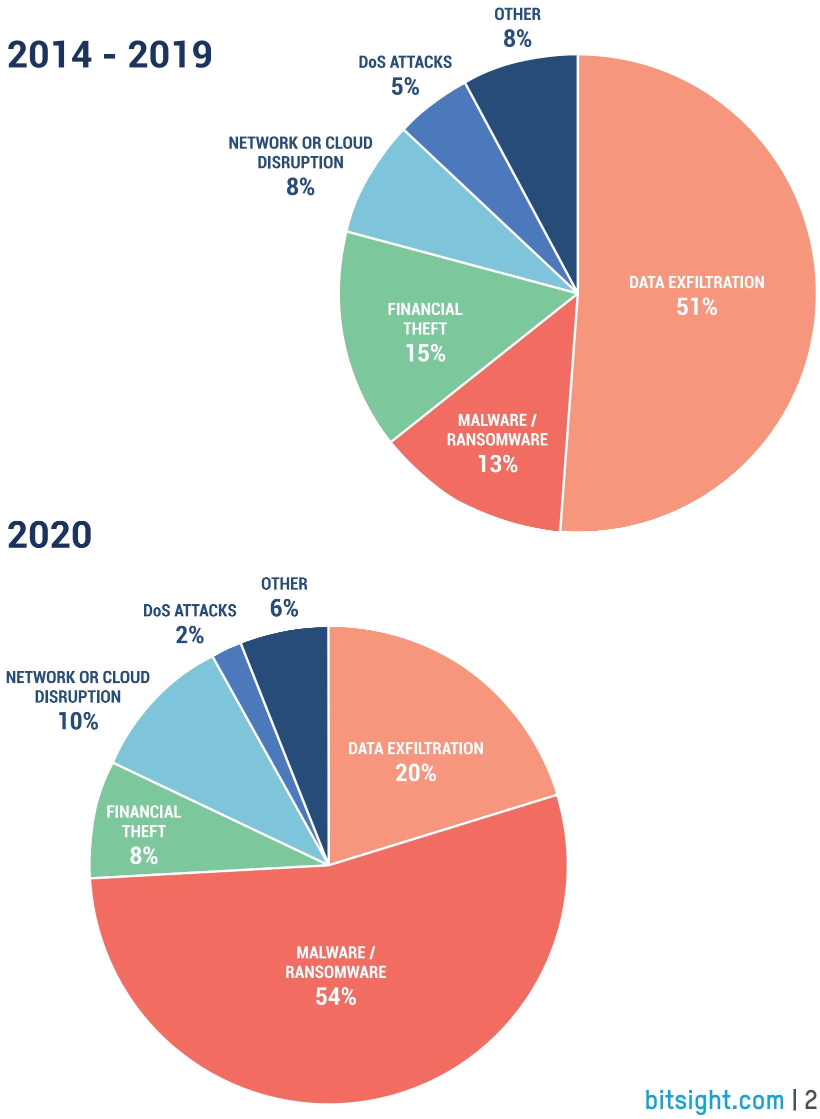
Ransomware: The Rapidly Evolving Trend

RANSOMWARE: THE RAPIDLY EVOLVING TREND

Looking back over recent years, ransomware has been an ongoing security threat for companies around the world. Digital transformation has accelerated — largely due to the rise in remote work resulting from the COVID-19 pandemic. Unfortunately, as companies went increasingly digital, a new opportunity emerged for cyber criminals to maximize profit by exploiting this new reality.

As seen in the below graphics, based on data collected by the University of Cambridge, ransomware cyber insurance claims have grown at an alarming rate over the past five years.

Cyber insurance claims by cause



2014 - 2019

2020

May 2021 proved that the ransomware trend is running ahead nearly unabated. In the United States, the Darkside APT group crippled the largest fuel supplier in the northeast, causing a system-wide shutdown affecting nearly the entire US east coast's fuel supply for several days. The REvil Group attacked JBS, a global meat supplier resulting in a similar shut down. In Europe, a double blow was dealt to the Irish health system when the Health Service Executive, Ireland's healthcare operator, and its Department of Health suffered a ransomware attack forcing a shutdown within its IT infrastructure.

- The health sector is regarded as particularly vulnerable to cyber incidents and crises. In the ENISA Threat Landscape report, it was found that more than 66% of healthcare organizations experienced a ransomware attack in 2019 — and 45% of attacked organizations paid the ransom. Of those organizations that paid the ransom, half still lost their data.
- In October 2020, the first case of triple extortion was seen in the real world. When a Finnish psychotherapy clinic, Vastaamo, was breached, attackers not only extorted the clinic to regain access to its files, but also to avoid the records being published — representing double extortion. The attackers went one step further by extorting individual patients regarding publishing their records.

In the chart below, you can see some of the latest tactics and victims of ransomware attacks:

Tactic	Extortion	Demand	Victims	Ransomware group
Encrypt	**Single**	Request payment for the encryption key	Colonial Pipeline (energy)	Darkside
			Düsseldorf University Hospital	To be determined
Exfiltrate	**Double**	Threaten public exposure of the data	Westech International (defense contractor)	Maze
			Blackbaud (cloud provider)	To be determined
	Triple	Threaten end customers / patients to avoid public exposure of the data	Vastaamo Clinic	To be determined
DDOS		Threaten a DDoS attack to bring the victim back to the negotiation table	AXA Asia	To be determined

Ransomware teams are evolving, and getting more and more sophisticated. With such a great potential to earn money, the so-called "ransomware gangs" have begun to be more organized and leverage defined business models. Many of their members have different roles, specializing in each one to maximize the gain, following a typical ransomware attack chain.

Campaign planning > Bait > Injection > Lateral movement > Infection > Extortion

As an example, Darkside (the team responsible for the attack on Colonial) follows a ransomware-as-a-service model, with ransomware payment demands that can range from $200,000 to $2,000,000. And this is a path that is starting to be followed by other ransomware operators, which appear to specifically target companies with an annual revenue of at least $1 billion.

The collateral consequences of ransomware also include the cost to insurance companies who underwrite cybersecurity policies. They conduct diligence in the form of questionnaires and assessments of an organization's cybersecurity performance data.

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 being victimized. Chief among them is a relentless focus on core security hygiene — with the goal of ensuring that security controls, practices, and team members are performing effectively every day. While best practices are widely acknowledged, it's clear that performance excellence is only being achieved by a few leaders.

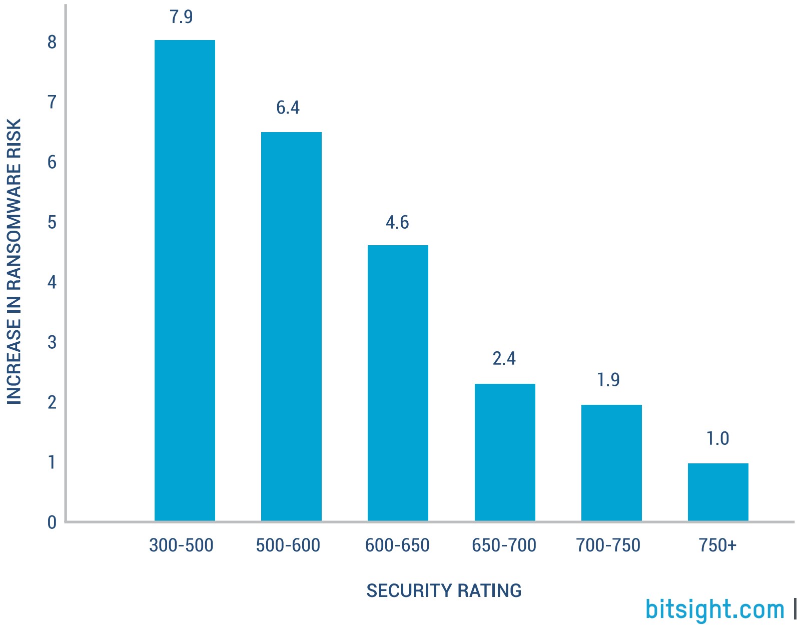
BitSight's research team analyzed hundreds of ransomware events since November 2018 to estimate the relative probability that an organization will experience a ransomware event. The analysis looked back over five six-month periods benchmarked against companies with a high BitSight Security Rating (750+) for security effectiveness.

Overall, the data shows that organizations with a rating lower than 600 are 6.4x, and organizations with a rating between 600-650 are 4.6x more likely to be a ransomware victim compared to the benchmark of organizations with a 750+ rating. BitSight continuously and non-intrusively assesses organizational cybersecurity performance by evaluating security performance observations across 23 different categories, including compromised and exposed systems, critical vulnerabilities, patching rates, software security, and other key issues.

BitSight processes more than 250 billion security measurements on a daily basis to provide an objective security rating (using a 250-900 scale) based on its observations that is independently verified to be correlated with breach risk.

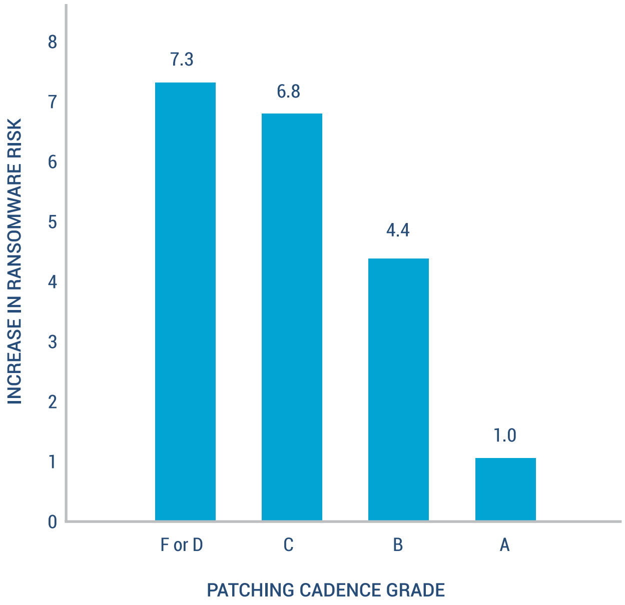
Risk Based on BitSight Rating

Increased likelihood of ransomware risk relative to organizations with a 750+ BitSight rating



Digging deeper into what BitSight calls individual risk vectors, patching cadence (the elapsed time between software patches becoming available compared to when patches are implemented) is a strong security program performance indicator. The more time that passes between patch available and patch implemented indicates lower performance. Unsurprisingly, poor patching performance correlates to a nearly sevenfold increase in ransomware risk for companies with a C grade or lower. TLS/SSL certificate and configuration management offer comparably strong security program performance indicators. Companies with a C grade or lower in TLS/SSL Configurations are nearly four times more likely to be a ransomware victim and companies with a C grade or lower in TLS/SSL Certificates are roughly three times more at risk of a ransomware incident.

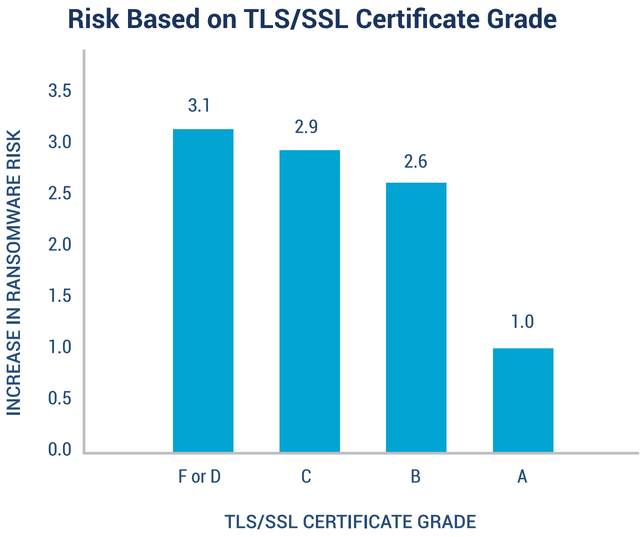
Risk Based on Patching Cadence Grade

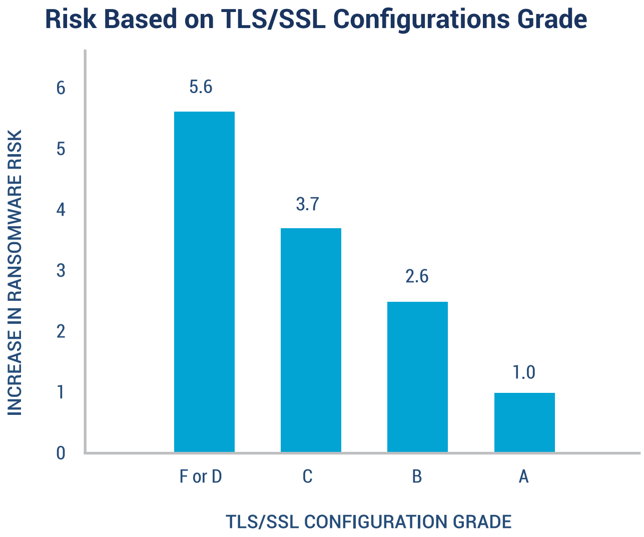


In the above chart and the two that follow, letter grades provide a quick way to understand how a company is performing in each risk type, as well as a meaningful way to compare risk type performance of one company to another.

Letter grades 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





Looking for a deeper understanding of the relationship between our security data and ransomware incidents, the BitSight data science team tested all the confirmed vulnerabilities used in the BitSight rating for correlation with ransomware incidents. Using a statistical analysis, they found five interesting cases where presence of a particular vulnerability indicated heightened risk of a ransomware incident.

Vulnerability	Increased Risk of Ransomware
CVE-2014-3566	1.5
CVE-2016-0800	1.3
CVE-2012-6708	1.3
CVE-2018-13379	1.8
PulseSecure Group	2.6

CVE-2014-3466 and CVE-2019-0800 are the Poodle and Drown SSL vulnerabilities, which are both related to obsolete SSL protocols and by themselves pose no serious threat to companies. However, tens of thousands of companies have been running servers that allow these obsolete protocols. Similarly, CVE-2012-6708 is an older jQuery vulnerability which is an unlikely attack vector and has been detected in nearly 20 thousand companies.

The vulnerability CVE-2018-13379 and a group of vulnerabilities associated with PulseSecure VPN devices are more interesting. CVE-2018-13379 is associated with Fortinet VPN devices and has a CVSS score of 9.8. For PulseSecure devices, there are seven vulnerabilities from 2019 which are often seen together; of these, CVE-2019-11510 is the most significant, having a CVSS score of 10.0 which is the highest possible value. Both of these vulnerabilities are very likely attack vectors and were specifically called out by US Government agencies: CVE-2018-13379 by DHS and CVE-2019-11510 by the NSA.

CONCLUSION

Overall the research demonstrates the correlation of BitSight's overall rating and performance against three risk vector ratings that provide clear ransomware risk indicators. Furthermore, analysis of specific vulnerabilities complements observations made regarding patching cadence resulting in increased ransomware risk.

The BitSight rating and three specific risk vectors provide strong ransomware risk indicators. Overall, the rating and risk vectors offer a statistically valid reflection of overall security practices. In other words, for organizations whose practice is to have long elapsed times between updates becoming available and patches implemented, this is very likely representative of practices in other security domains. Therefore, while rating and risk vectors offer specific evidence, the elevated ransomware risk will simply shrink by improving patching cadence. Risk reduction will come from an overall improvement in practices.

Regarding vulnerabilities, BitSight data concludes that there are two main possibilities for the correlation between the select vulnerabilities and the likelihood of suffering a ransomware event:

- **Hygiene matters.** Presence of the described vulnerabilities is an indicator of security performance for an organization. This is especially true for older vulnerabilities that should have been patched long ago, and 11 of the 17 vulnerabilities have CVE dates from 2018 and older. Organizations that fail to patch vulnerabilities older than two years (and one could argue, older than a few weeks) have gaps in governance, operations, management, asset inventory, or other fundamental IT management and security practices.

- **Certain vulnerabilities matter.** Ransomware used to be delivered mainly through phishing attacks; however, modern, large-payment demands often abuse recent vulnerabilities in widely deployed technology that will yield them easy access to the target's infrastructure. These include the vulnerabilities in Fortinet, Citrix, and Pulse Secure (CVE-2020-11510), all of which may give attackers access to a perimeter security gateway.

The research demonstrates how daily security program performance matters. As organizations deploy anywhere from 20 to 50 discrete security controls, leadership teams everywhere are asking the question, "Is my organization protected?" The answer is not about how much you spend, but rather how diligently controls are maintained. Cyber attacks rarely employ novel, never-before-seen techniques, like zero day attacks. It is far more common for attackers to acquire customizable tools available on the dark web to exploit a series of vulnerabilities and weak controls to wreak havoc.

BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Seven of the top 10 largest cyber insurers, 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit **www.BitSight.com**, read our blog or follow **@BitSight** on Twitter.