BitSight's Analysis of Sector - Specific Ransomware Risk

Joe Lyons; senior director, signals and ratings research; BitSight
John Adams; cyber risk analyst; BitSight

BITSIGHT®
The Standard in SECURITY RATINGS

TABLE OF CONTENTS

Ransomware

Ransomware is a type of malicious event where attackers encrypt an organization's data and demand payment to restore access. Attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. [1]

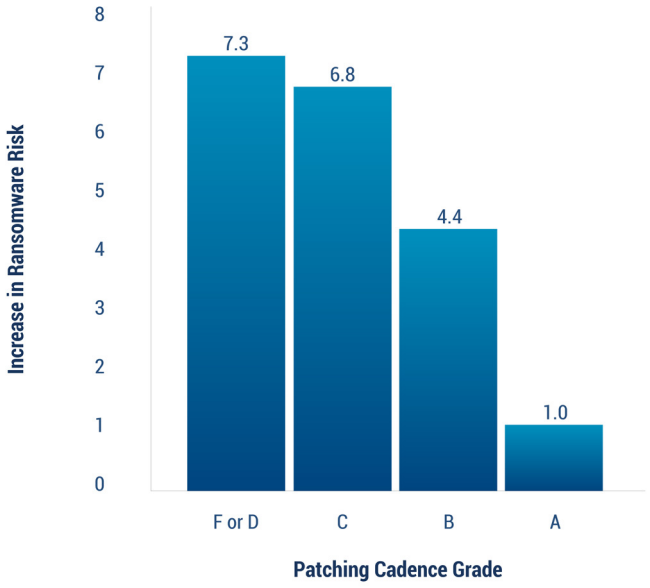
THE PROBABILITY OF A RANSOMWARE EVENT

This paper expands on earlier BitSight analysis of ransomware probability to allow for the creation of a heat map providing relative sector rankings. This type of ranking provides an easy-to-use framework for analysts across finance, credit, and insurance to inform risk decisions at the sector level. As such, quartiles were created by examining a binary measure: "is this organization at an increased risk of ransomware, or not?" This approach was applied to over 300,000 organizations' security performance risk vectors, as measured by BitSight. Once the binary measure was examined, the data were organized into sectors and performance quartiles were created. BitSight showed that three risk vectors – Patching Cadence, TLS/SSL configurations, and TLS/SSL certificates – displayed the strongest correlation to an organization's increased likelihood of experiencing a ransomware event. The BitSight study "Evidence-Based Strategies to Lower Your Risk of Becoming a Ransomware Victim" showed that the grades listed correlate to an increased likelihood that a company will experience a ransomware event.

The following is a summary of the findings from this earlier research:

PATCHING CADENCE

Measures how many systems within an organization's network are affected by important vulnerabilities, and how quickly the organization remediates them.

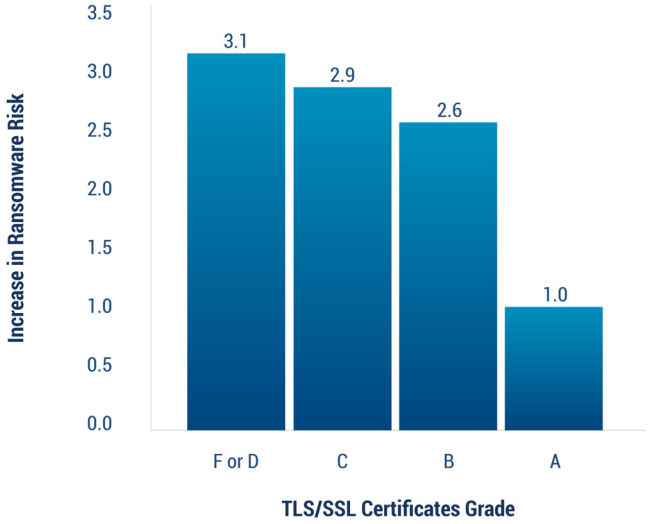


The above figure shows A as the baseline; B is a 4.4x increase; C is a 6.8x increase; and D or F is a 7.3x increase in the likelihood of experiencing a ransomware event.

[1] *NISTIR 8374, Ransomware Risk Management: A Cybersecurity Framework Profile | CSRC*

TLS/SSL CERTIFICATES

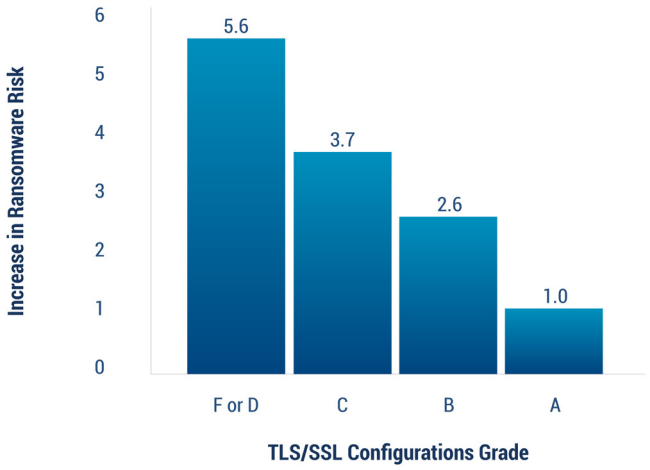
Measures whether a company has properly obtained and deployed TLS/SSL encryption certificates that are used to secure communication over the Internet.



The above figure shows A as the baseline; B is a 2.6x increase; C is a 2.9x increase; and D or F is a 3.1x increase in the likelihood of experiencing a ransomware event.

TLS/SSL CONFIGURATIONS

Measures whether a company has correctly configured security encryption software and whether that software utilizes strong encryption protocols when making encrypted connections to other machines.



The above figure shows A as the baseline; B is a 2.6x increase; C is a 3.7x increase; and D or F is a 5.6x increase in the likelihood of experiencing a ransomware event.

METHODS

COMPARING RELATIVE SECTOR RANSOMWARE RISK

To compare the relative risk of ransomware by sector, BitSight counted the proportion of companies scoring lower than an "A" on Patching Cadence, TLS/SSL configurations, and TLS/SSL certificates within each sector. Lower scores in these risk vectors were demonstrated by BitSight to correlate with a higher risk of ransomware. Once the proportion of companies per sector scoring lower than an "A" were calculated, the sectors were organized into quartiles and given a rank between 1 and 4. This ranking allows for a relative comparative analysis of which sectors had the highest proportion of companies at an increased risk of ransomware events based on BitSight's vectors.

Below, we provide an illustrative example calculation focusing on only one risk vector, Patching Cadence. For demonstration purposes, all values and sector descriptions in this section are fictitious.

	Sector X	Sector Y	Sector Z	Sector Q
Patching cadence grades by company	A: 3 B: 2 C: 4 D/F: 1	A: 1 B: 3 C: 1 D/F: 1	A: 3 B: 1 C: 2 D/F: 0	A: 1 B: 5 C: 10 D/F: 3

The relative proportion of the increased risk is then calculated with the following method:

$$p = \frac{\textit{Companies in Sector Scoring less than A}}{\textit{Total Number of Companies in Sector}}$$

Where:

p = Proportion of companies in sector at an increased ransomware risk due to the risk vector in question (in this example, BitSight's Patching Cadence risk vector).

This method allows for a relative comparison of the risk sectors by sector as follows:

	Sector X	Sector Y	Sector Z	Sector Q
Proportion of companies in sector at an increased risk of ransomware due to a B or lower Patching Cadence grade	.70	.83	.50	.95

[2] *BitSight Security Ratings Correlate to Ransomware*

Once the proportion of companies at an increased risk of a ransomware event is calculated per sector for the risk vector in question (again, Patching Cadence in this example), quartiles are formed using the ranges observed in the results. The sector quartiles are calculated using the following formulas:

Pythonic pseudocode

Q1 = np.percentile([dataset], 25)
Q2 = np.percentile([dataset], 50)
Q3 = np.percentile([dataset], 75)

The quartile values are as follows:

Calculated Quartiles

Q1	0.65
Q2	0.765
Q3	0.86

Using the quartile values shown above, each sector is given a rank value depending on where it falls in the quartile range.

Proportion to Quartile to Rank

Proportion of entities in sector with increased risk (p)	Quartile	Rank
$p < 0.65$	1	1
$0.65 \leq p < 0.765$	2	2
$0.765 \leq p < 0.86$	3	3
$p \geq 0.86$	4	4

Finally, projecting each sector's rank back into the quartiles ranking table looks as follows:

	p	Quartile Rank
Sector Z	0.50	1
Sector X	0.70	2
Sector Y	0.83	3
Sector Q	0.95	4

RESULTS

SECTORS EXAMINED

RELATIVE RISK MATRIX

SECTOR	Average Rank	Patching Cadence	TLS/SSL Certificates	TLS/SSL Configurations
Aerospace/Defense	4	4	4	4
Education	4	4	4	4
Government/Politics	4	4	4	4
Telecommunications	4	4	4	4
Transportation	4	4	3	4
Utilities	4	4	4	3
Consumer Goods	3	3	3	2
Energy/Resources	3	3	4	3
Manufacturing	3	2	3	3
Media/Entertainment	3	3	2	3
Retail	3	3	3	4
Technology	3	2	3	3
Engineering	2	2	2	2
Food Production	2	3	2	2
Real Estate	2	1	2	2
Tourism/Hospitality	2	2	2	2
Business Services	1	1	1	1
Credit Union	1	1	1	1
Finance	1	1	2	1
Healthcare/Wellness	1	1	1	2
Insurance	1	2	1	1
Legal	1	1	1	1
Nonprofit/NGO	1	2	1	1

CONCLUSION

By examining each sector's performance across the three BitSight risk vectors found to be correlated to ransomware probability, we established a relative sector ranking that measures the proportion of organizations within a sector at an increased risk of ransomware. The risk vectors examined in this study are (1) Patching Cadence, (2) TLS/SSL configurations, and (3) TLS/SSL certificates.

When examining sector performance for patching cadence, the top three performing sectors are credit unions, business services, and legal; the proportion of companies found to achieve a grade of less than an "A" is 0.20, 0.20, and 0.21, respectively. The sectors performing the worst with respect to patching cadence were government, education, and telecommunications; the proportion of companies found to achieve a grade of less than an "A" is 0.34, 0.38, and 0.46, respectively.

With respect to TLS/SSL Certificates, the top three performing sectors are legal, nonprofits, and credit unions; the proportion of companies that were found to achieve a grade of less than an "A" were all 0.36, 0.36, and 0.37, respectively. The sectors performing the worst with respect to TLS/SSL Certificates were utilities, education, and telecommunications; the proportion of companies found to achieve a grade of less than an "A" is 0.48, 0.51, and 0.69, respectively.

Finally, studying TLS/SSL Configurations, the top three performing sectors were credit unions, insurance, and finance; the proportion of companies found to achieve a grade of less than an "A" is 0.54, 0.61, and 0.62, respectively. The sectors performing the worst with respect to TLS/SSL Configurations are education, government/politics, and telecommunications; the proportion of companies found to achieve a grade of less than an "A" is 0.73, 0.74, and 0.83, respectively.

Perhaps the most interesting insight that can be gleaned from this analysis is the average of the quartile rankings for each vector. To derive the average, all three quartile scores were summed and divided by 3. The most notable top performers were finance and business services, both of which have a high level of digitization and an average quartile rank of 1. The most notable poor performers were utilities, education, and government/politics. These sectors all represent high systemic risk sectors and all score a 4 for the average quartile ranking.

As sector digitization increases, each sector's ability to protect against cyber risks must also increase. Highly digital sectors such as finance, technology, and business services must continue to invest in cybersecurity to set the tone for defense in the remaining sectors.

REFERENCES

1. "BitSight Security Ratings Correlate to Ransomware;" BitSight; https://www.bitsight.com/sites/default/files/2022-03/2022%20BitSight%20Security%20Ratings%20Correlate%20to%20Ransomware.pdf ; Accessed 13 June 2022.
2. "Evidence-Based Strategies to Lower Your Risk of Becoming a Ransomware Victim;" BitSight; https://www.bitsight.com/blog/ransomware-prevention ; Accessed 13 June 2022.

ABOUT BITSIGHT

BitSight transforms how organizations manage cyber risk. The BitSight Security Ratings Platform applies sophisticated algorithms, producing daily security ratings that range from 250 to 900, to help organizations manage their own security performance; mitigate third-party risk; underwrite cyber insurance policies; conduct financial diligence; and assess aggregate risk. With the largest ecosystem of users and information, BitSight is the Standard in Security Ratings. For more information, please visit **www.bitsight.com**

OUR OFFICE LOCATIONS

BOSTON (HEADQUARTERS)
111 HUNTINGTON AVE
SUITE 2010
BOSTON, MA 02199, USA
PHONE: +1-617-245-0469

RALEIGH
510 GLENWOOD AVE, SUITE 301
RALEIGH, NC 27603, USA

LISBON (EMEA HEADQUARTERS)
CENTRO EMPRESARIAL ESPAÇO 7 RIOS
ESCRITÓRIO 50 (0.04), PISO -1
RUA DE CAMPOLIDE, Nº 351
1070-034 LISBON, PORTUGAL
PHONE: +351 217252110

ISRAEL
TOTZERET HAARETZ ST. 7
4TH FLOOR
TEL AVIV-YAFO, ISRAEL

SINGAPORE
7 TEMASEK BOULEVARD
LEVEL 32 SUNTEC TOWER 1
SINGAPORE 038987

FOLLOW US ON:

BITSIGHT
The Standard in SECURITY RATINGS