BITSIGHT
The Standard in SECURITY RATINGS

thirdpartytrust

EBOOK

Ransomware in the Utilities Sector

RANSOMWARE IN THE UTILITIES SECTOR

Ransomware is an epidemic. How can security professionals in the Utilities sector reduce the risk of becoming a ransomware victim? Which practices are effective in minimizing risk?

BitSight recently analyzed hundreds of ransomware incidents over the last three years — including those impacting the Utilities sector — to identify common security performance gaps and challenges that lead to successful ransomware incidents. Based on our analysis, we find that certain security program practices may be critical to reduce the likelihood of experiencing a ransomware incident. We also identify which vulnerabilities are closely tied with ransomware campaigns.

This report contains our key findings for the Utilities sector. It is our hope that these findings are useful to your organization to avoid future ransomware incidents. If you would like specific information about your organization, please contact us at: www.bitsight.com

RANSOMWARE: A GLOBAL EPIDEMIC

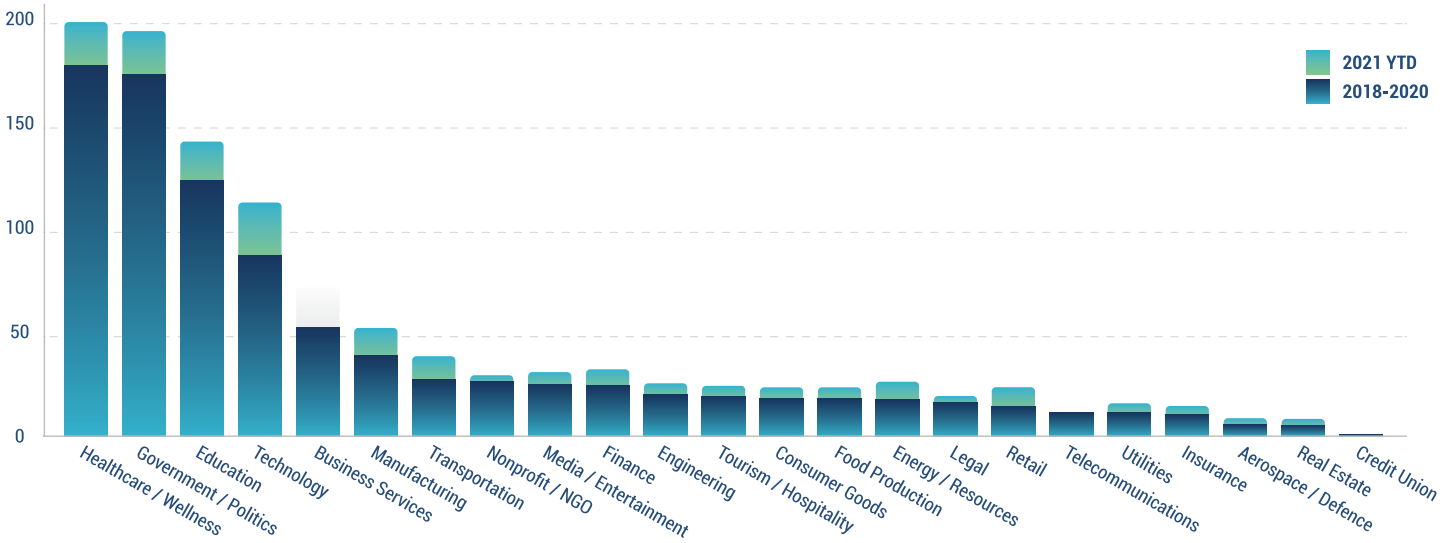
2021 has been dominated by ransomware. Numerous high-profile incidents around the globe have shed light on the damaging impact that ransomware can have on individual organizations and global supply chains.

In the U.S., the largest fuel supplier in the northeast was crippled by a ransomware attack, causing a system wide shutdown affecting nearly the entire U.S. east coast fuel supply for several days. Weeks later, an attack targeting a meat processing plant disrupted food supply. In Europe, a double whammy hit the Irish health system when the Health Service Executive, Ireland's health care operator, and its Department of Health suffered a ransomware attack forcing a shutdown within the IT infrastructure. Incidents continue to hit the news at an alarming rate.

Are ransomware incidents actually increasing, or are they just becoming more public? Data suggests that ransomware attacks have indeed increased dramatically over the last year. Law enforcement officials state that while there have been hundreds of publicized ransomware incidents, just as many have taken place behind closed doors. Insurers report that ransomware-related incidents are on the rise; insurance broker Aon finds that ransomware attacks have increased 486% over the past two years, resulting in significant financial losses for organizations globally. According to a recent Cambridge University study, ransomware insurance claims represented more than half of cyber insurance claim losses in 2020.

BitSight data confirms that the number of successful ransomware incidents is indeed increasing across all organizations, all sizes, and all sectors but not equally. When it comes to publicly disclosed ransomware incidents, we continue to find that Healthcare, Government, Higher Education, and Technology are the sectors who experience ransomware incidents at the highest rates.

Ransomware Incidents by Sector, 2018-2021 (Source: BitSight)



Why is ransomware growing so rapidly? It's all about the money. It is now typical for criminals to obtain multiple ransomware payments from the same victim. No longer limited to soliciting one-time payments for decrypting data, criminals now threaten to exfiltrate company data or perform denial of service (DDOS) attacks against organizations who do not meet demands for double and triple payments. It is no wonder that ransomware attacks are expected to cost organizations more than $265 billion over the next decade.

DATA ANALYSIS OF RANSOMWARE VICTIMS

With so much attention and focus on ransomware coming from the C-suite and boardroom, security professionals are focusing their efforts on how to reduce the likelihood that they will experience an incident now more than ever. But what practical steps can security professionals in the Utilities sector take?

BitSight's research team analyzed hundreds of ransomware events since Nov 2018 to estimate the relative probability that an organization will experience a ransomware event. We wanted to understand if particular security practices — or lack thereof — may be leading indicators of experiencing a ransomware incident.

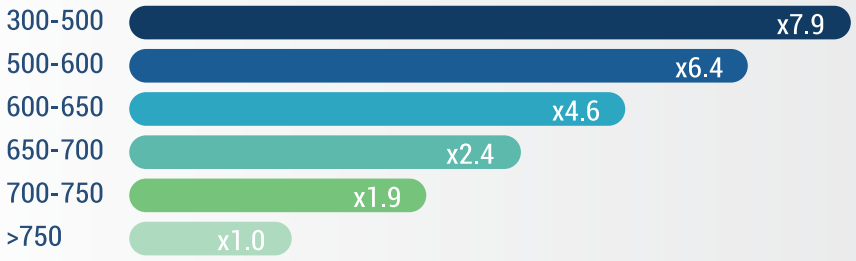
Our analysis looked back over five six-month periods benchmarked against companies with high BitSight Security Ratings (750+), indicative of security effectiveness. By comparing the security performance of those who have been impacted by ransomware against those who have not, we have identified a number of critical performance indicators that may be useful to help security professionals in the Utilities sector reduce the risk of becoming a ransomware victim.

INCREASED LIKELIHOOD OF RANSOMWARE BASED ON OVERALL SECURITY PERFORMANCE

Overall, the data shows that organizations with weaker overall security performance are more likely to experience a ransomware incident. BitSight continuously and non-intrusively assesses organizational cybersecurity performance by evaluating externally-observable security performance issues 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), following a similar approach followed by credit rating agencies, based on its observations that is independently verified to be correlated with breach risk.

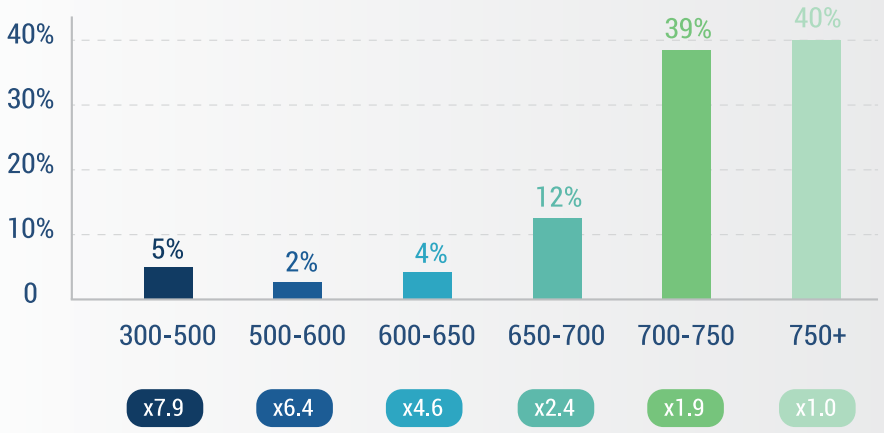
We find that organizations with a security performance rating lower than 600 are 6.4x, and organizations with a rating between 600-650 are 4.6x more likely to be a ransomware victim compared to the benchmark of organizations with a 750+ rating.

Probability of Experiencing Ransomware Based on the BitSight Rating



We apply this analysis to the Utilities sector to understand how Utilities companies are performing and their risk of ransomware. Overall, nearly 40% of Utilities sector organizations have a 750+ rating, making them less likely to experience a ransomware attack. This means that 60% of the Utilities sector is at heightened risk of ransomware.

Probability of Experiencing Ransomware in the Utilities Sector (Based on BitSight Rating)



HOW PATCHING CADENCE IMPACTS RANSOMWARE RISK

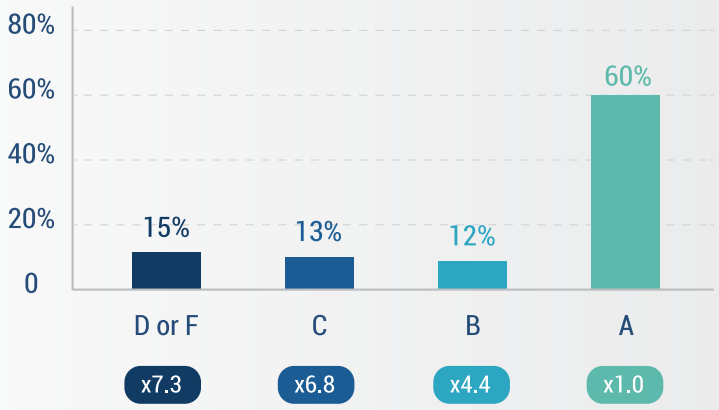
Are there certain security program controls that are a stronger indicator of ransomware risk? One area that we researched is "Patching Cadence," the elapsed time between software patches becoming available compared to when patches are implemented. BitSight measures an organization's Patching Cadence rate by examining the presence and duration of high-confidence vulnerabilities observed on a company's infrastructure. BitSight's analysis considers vulnerabilities across all severity types - from moderate to critical.

We find that Patching Cadence is a strong overall security program performance indicator. The more time that passes between patch available and patch implemented indicates lower performance. Unsurprisingly, poor patching performance also correlates to an increase in ransomware risk. Companies who are a "B" in patching cadence are 4.4x more likely to experience ransomware; a "C" grade or lower makes an organization nearly 7x more likely to experience ransomware.

Probability of Experiencing Ransomware Based on Patching Cadence

We apply this analysis to the Utilities sector to understand how Utilities companies are performing on patching systems. Overall, nearly 60% of Utilities sector organizations have an "A" in Patching Cadence, making them less likely to experience a ransomware attack. But 13% are at "C" or below, and 15% are in the "D" or "F" range when it comes to patching cadence. This means that approximately 41% of the Utilities sector is at heightened risk of ransomware.

Probability of Utilities Organizations Experiencing Ransomware Based on Patching Cadence



SPECIFIC VULNERABILITIES AND RANSOMWARE RISK

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

	VULNERABILITIES
1.5x	POODLE (CVE-2014-3466)
1.3x	DROWN (CVE-2016-0800)
1.3x	CVE-2012-6708
1.8x	CVE-2018-13379
2.6x	PULSE SECURE GROUP

CVE-2014-3466 and CVE-2016-0800 are the Poodle and Drown SSL vulnerabilities. These 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 20,000 companies around the globe.

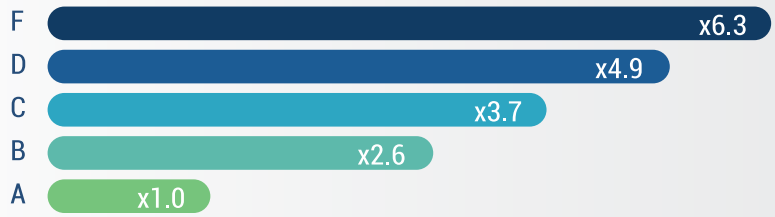
The vulnerability CVE-2018-13379 and a group of vulnerabilities associated with PulseSecure VPN devices are more threatening. CVE-2018-13379 is associated with Fortinet VPN devices and has a CVSS score of 9.8. For PulseSecure devices, there are seven vulnerabilities from 2019 which are often seen together; 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 U.S. Government agencies: CVE-2018-13379 by Department of Homeland Security and CVE-2019-11510 by the National Security Agency.

CERTIFICATE/CONFIGURATION MANAGEMENT AND RANSOMWARE RISK

TLS/SSL certificate and configuration management offer comparably strong security program performance indicators. BitSight determines if the security protocol libraries support strong encryption standards when making connections to other machines. Incorrect or weak TLS/SSL configurations result in infrastructure becoming vulnerable to potential attack.

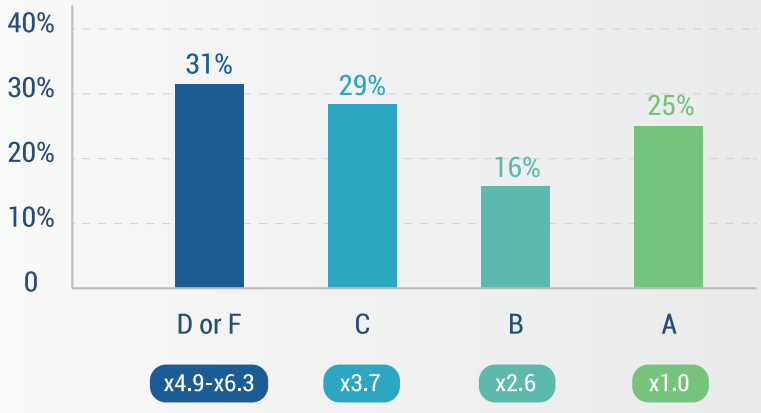
Companies with a C grade or lower in TLS/SSL Configurations are nearly four times more likely to be a ransomware victim. We also find increased risk in ransomware regarding TLS/SSL certificate management. Companies with a C grade or lower in managing TLS/SSL Certificates are roughly three times more at risk of a ransomware incident

Probability of Experiencing Ransomware Based on TLS/SSL Configurations



We apply this analysis to the Utilities sector to understand how Utilities companies are performing on addressing configuration issues. Overall, nearly 25% of Utilities sector organizations have an "A" in TLS/SSL Configurations, making them less likely to experience a ransomware attack. But 29% are at "C", and 26% are in the "D" or "F" range when it comes to configuration management. This means that more than 75% of the Utilities sector is at heightened risk of ransomware.

Probability of Utilities Organizations Experiencing Ransomware Based on TLS/SSL Configurations



NEXT STEPS: WHAT CAN UTILITIES SECTOR SECURITY PROFESSIONALS DO?

As the ransomware epidemic continues, security professionals must put their organizations in the best position to mitigate the likelihood of a catastrophic incident. We know that while no organization is immune from experiencing a cyber incident, there are best practices for minimizing the likelihood of being victimized.

The growing risk of cyber compromise requires a stronger, more consistent, and comprehensive approach. Measuring and maintaining ongoing security performance across the entire ecosystem is critical to defending against the next cyberattack. Maintaining strong cybersecurity performance isn't about checking a box, but about day-to-day security performance efficacy and proper risk management. Sound security performance management over time – including moving beyond point in time practices toward continuous testing – creates cyber-resilient businesses, and is the key to organizations within the Utilities industry improving their cybersecurity capabilities.

Proper enterprise cyber risk management requires organizations to address security within their own environments and throughout their digital ecosystem. Utilities sector security professionals can prepare themselves by understanding their performance in these particular areas of concern.

Your own security performance isn't all you need to worry about – cybersecurity hygiene also extends to your partners, suppliers, and any third-party member of your network. Cybercriminals are able to find and attack the least secure business in the supply chain and use that foothold to gradually compromise their partners. Having tools that provide deep insight into the risks and security performance of every member of your supply chain is critical. Business leaders can use this data to make informed decisions about which organizations they choose to do business with, how they transact, and ultimately how to defend the network.

BitSight can help you manage risk during these challenging times. Please reach out to a BitSight representative for your custom Benchmark Report or Third Party Risk Assessment, which highlights specific areas of risk within your organization and throughout your third party supply chain.

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.