Detected and Prevented

Known Attacker Log

virsec™

Stop Ransomware and Zero-day Attacks with True Runtime Protection

Article after article, every day we seem to hear of another successful ransomware attack against a public or private institution. In fact, the numbers are much higher with research showing **2,084 ransomware attacks in the U.S. in the first half of 2021 alone—a 62% increase from the same period in 2020[1].** And these are just complaints reported to the FBI. The truth is ransomware attacks have been going on for years, and we even see the same organizations falling victim multiple times.

So, why is ransomware on the rise and such a challenge to protect against these zero-day attacks? Here, we'll examine some of the key factors that contributed to the rise of ransomware attacks as well as recent initiatives and innovations that enable defenders to better mitigate risk and stop attacks before they start.

Ransomware is Big Business

If Ransomware were a Silicon Valley start-up, it would be considered a "Unicorn": high growth, high reward, low risk, minimal competition. Ransomware techniques are often successful, and the perpetrators are rarely prosecuted. When combined with the emergence of Bitcoin and other cryptocurrencies as means for payment; cybercriminals are difficult to trace. As a result, ransomware attacks are escalating and becoming more sophisticated and evasive.

Since the COVID-19 pandemic, ransomware has burgeoned into a multi-billion-dollar industry. As extortionists seek out larger and larger scale operations in search of an ever-multiplying bounty, more and more businesses and industries are at risk. In 2021, for the first time, attackers were successful in shutting down critical infrastructure in the U.S., including Colonial Pipeline, the East Coast's largest gasoline, diesel, and natural gas distributor, and JBS, the world's largest meat processor. Initial demands for payment are reaching new heights—exceeding 10 million dollars and sometimes as high as **40 to 60 million**—for targets with deep pockets.[2] However, threat actors aren't just setting their sights on multinational enterprises. Plenty of cities and counties across the country have been extorted as well.

While ransom is the most obvious revenue stream for threat actors, ransomware-as-a-service (RaaS) is unlocking additional sources of revenue for a host of participants in this underground economy. Highly skilled cybercriminals develop and sell their capabilities to malicious actors who don't have the resources to develop these tools on their own. All participants supporting the service—those that provide encryption tools, communications, technical support, training, and ransom collection—share in the profits. Payment models vary and might consist of pure profit sharing, a monthly subscription fee with or without profit sharing, or a one-time licensing fee.

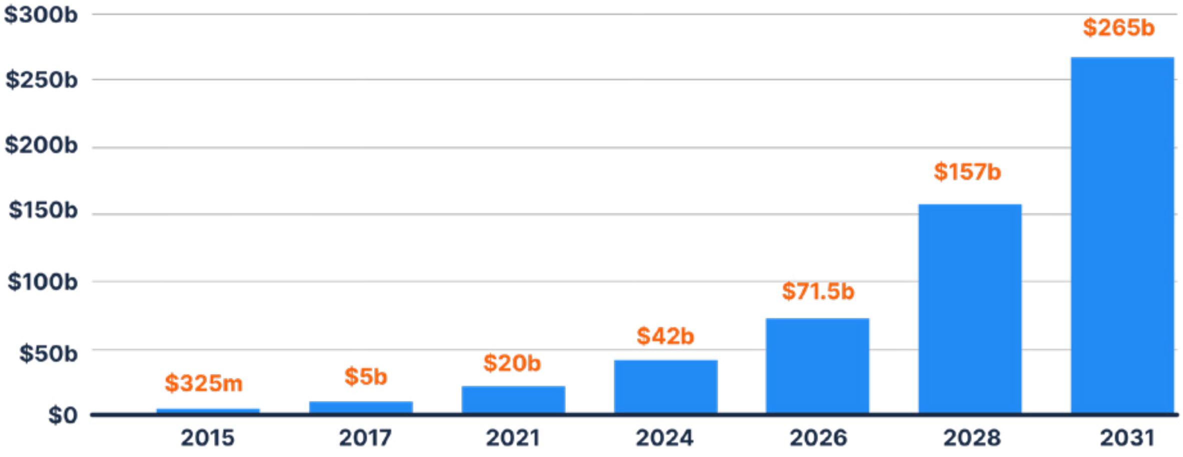
Ransomware demands were **up by 225%** in 2020.[3]

Costs Beyond the Ransom

When ransomware attacks happen, the ransom payouts usually make the headlines. However, the total financial impact of a successful attack on an organization is even more sobering. Collective global ransomware costs to businesses for 2021 are estimated to exceed $20 billion.[4]

Damages include not just the ransom payment (if made), but other costs in connection to these attacks, like **detection and escalation, lost business, notification, and post breach response.** In a year when the average total cost of a data breach increased nearly 10% from the previous year, the average total cost of a ransomware breach jumped even higher and has now reached $4.62 million, costlier than any other type of breach.[5] Full recovery can take weeks if not months and can be far more complicated than anticipated, even if organizations appear to be back online within a few days.

Projected ransomware damages[6] are projected to increase significantly over the next 10 years:



A Multi-Faceted Challenge

If we take a closer look at why ransomware is proliferating, we can see that it is a multi-faceted challenge. Attacks can be executed in a matter of seconds and leverage a wide range of techniques to break into systems, access sensitive data, hijack operations, deploy encryption tools, encrypt data, and demand a ransom.

Ransomware Is Instantly Weaponized

Ransomware is so destructive because it can be instantly weaponized. It does not require any form of reconnaissance, any form of lateral movement, or privilege escalation. Threat actors don’t have to know where they are in your environment or understand what’s of value. They simply encrypt everything, and it’s irreversible without the key.

Ransomware is most damaging when it moves laterally from desktops to servers, which are online 24/7/365 and house all the critical applications and data necessary to keep an organization operational. On the server workload, malicious code that executes undetected during runtime can do the most damage. **It reaches deep into the inner architecture** of applications and targets the entire function. This includes the full data set and resources and more broadly, entire server workloads. Once deployed, **ransomware can encrypt files and block access.**

On the server workload, malicious code that executes undetected during runtime **can do the most damage.**

Unfortunately, more than 75% of companies infected with ransomware are using endpoint protection products (EPP) or endpoint detect and response (EDR) tools that they believe could help mitigate risk.[7] However, EPP/EDR tools are not fully equipped to protect against ransomware that can bypass conventional, probabilistic tools like these. Tactics based on endless threat chasing and trying to seal off porous perimeters have proven to be ineffective.

Commonly Used Ransomware Techniques

In 2020, ransomware surged to grab the third spot in types of actions associated with breaches, more than doubling its frequency from 2019.[8] Initial infiltration is achieved through a variety of techniques, exploiting web-based attacks such as SQL injection, or stealing credentials through phishing or other various social engineering methods. A majority (60%) of ransomware cases in 2020 involved direct install or installation of the ransomware through desktop sharing applications. The remainder of cases involved email, network propagation or download by other malware. Servers are **primarily targeted because that's where the data is located.**[9]

As organizations setup data backup solutions to mitigate these attacks, threat actors evolved their tactics as well. Now, 81% of ransomware attacks involve the threat to leak exfiltrated data, if the victim doesn't pay the ransom.[10] Depending on the type of data exposed, the leak can compromise digital intellectual property (IP) and erode customer trust and loyalty, unless the ransom is paid.

The Defender's Dilemma: To Pay or Not to Pay?

Victims of ransomware face a difficult choice. Either pay the ransom and hope to restore their vital data, or risk never recovering any of it. Even if they do recover their data, there is no guarantee it will be intact or not damaged. One study found that only 8% of organizations manage to retrieve their data after paying a ransom, and 29% of organizations received less than half of their data.[11]

As to how many victims pay, the data ranges widely across private versus public targets and across enterprise organizations themselves—from nearly a third[12] to closer to 70%[13] paying a ransom to regain data. Adding insult to injury, almost 80% of organizations that pay ransoms are hit again with another ransomware attack. Nearly 46% of the recurring attacks were from the **same group that executed the first attack.**[14]

Nearly 80% of organizations that pay ransoms are hit again with another ransomware attack. Nearly 46% of the attacks were from the same group that executed the first attack.

However, for some organizations the decision to pay or not to pay may soon be out of their hands. States, including New York, North Carolina, and Pennsylvania, are considering legislation that **would ban state and local government agencies from paying ransom.** They argue that prohibiting payments would deter attacks. But some experts point out that attacks will still happen as cybercriminals aren't going to research state laws and back off accordingly. And restoring and rebuilding systems could prove more costly and time consuming, particularly for smaller local governments. Instead of inadvertently further penalizing victims, providing aid to enable better protection is a more effective approach.[15] Many cities are underfunded, but even if the budget is there, **cities struggle to retain skilled cybersecurity talent.**

Only
8%
of organizations manage to retrieve their data after paying a ransom.

29%
of organizations received less than half of their data.

The Role of Cyber Insurance

Cyber insurance is becoming an increasingly popular risk mitigation strategy. Most policies cover costs to investigate a ransomware attack, negotiate with hackers, and make a ransom payment. So, it comes as no surprise that the number of companies opting for cybersecurity coverage grew **from 26% in 2016 to 47% in 2020.**[16]

However, some research suggests that this practice is encouraging cybercriminals. Insurers are not using incentives to reward better security practices or imposing higher fees or penalties for those who fail to improve security practices. Cybercriminals know that companies that have insurance are quick to pay the ransom. They even infiltrate insurance companies to seek customers' identities and scope of coverage so they can target them.

Challenges with gathering data to inform underwriting and risk modeling also make it difficult to accurately price policies. And, larger-scale attacks such as the SolarWinds supply chain breach are generating tremendous losses for the industry and leaving many insurers wondering if the offering is sustainable. While most companies **have seen a rise in premiums by up to 30%,**[17] the financial stakes are still too high for some insurers, jeopardizing the availability of coverage.

As companies look to renew policies, and first-time customers explore their options, they may encounter reimbursement limits, deductibles, as well as strict requirements for better cybersecurity strategies. It's becoming increasingly clear that cyber insurance is not a silver bullet solution to protect organizations, but instead should be viewed as one part of a risk mitigation strategy that must include best practices, compensating controls, and advanced ransomware protection.

> The Federal Bureau of Investigations (FBI) and the Cybersecurity and Infrastructure Agency (CISA) strongly discourage companies from paying ransoms to criminal actors, **but companies often have little choice.**

Will the U.S. Government Help?

In the U.S., the Federal Bureau of Investigations (FBI) and the Cybersecurity and Infrastructure Agency (CISA) strongly discourage companies from paying ransoms to criminal actors, but companies often have little choice. Many feel it is better to pay and hope they will be able to resume operations quickly rather than engage in a long shutdown. **So, the U.S. government is bringing its sizeable resources to bear on the problem.**

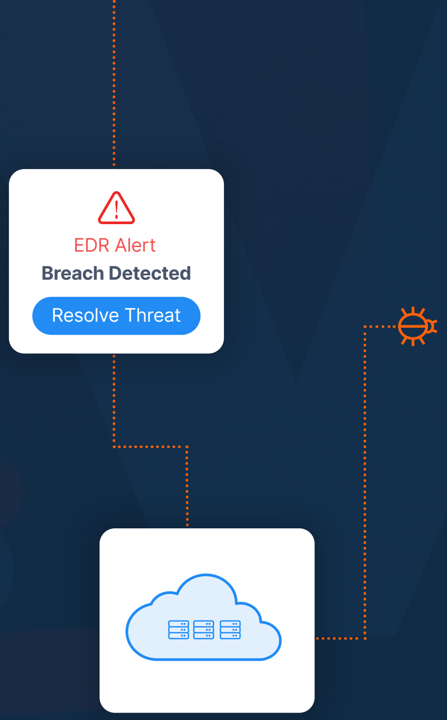
In the wake of the Colonial Pipeline attack and the White House Executive Order on Improving the Nation’s Cybersecurity issued in May 2021, the U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority to terrorism. The U.S. attorney’s offices will be expected to share updated case details and active technical information with leaders in Washington. The move encourages reporting and tracking of associated activities to accelerate detection and response of large-scale ransomware activity.

The Biden administration has also announced the creation of a **multiagency task force to combat ransomware** and launched a new website to help companies and government agencies better protect themselves. The site includes detailed guidance and tips for dealing with ransomware, frequently asked questions, and an extensive library of resources. A link to report ransomware incidents to the U.S. government makes it easy to report once, and all relevant agencies will be notified.

In a move to encourage collaboration between government industry, **the White House hosted a cybersecurity summit with several major technology companies** and announced a series of initiatives designed to help solve the ransomware crisis. These include better integrating cybersecurity into products, improving cybersecurity training, and developing a new framework for improving cybersecurity for technology supply chains.

Pushing the conversation even further, the next step is to involve more companies, bringing the full extent and power of industry insights and innovation to address the problem. As former Cisco Chairman and CEO John Chambers said, “The startups are where the innovation happens.”[18] Public and private enterprises have an obligation to think bigger, innovate faster and, ultimately, evolve our collective approach to this scourge of ransomware attacks.

A New Era: Continuous Runtime Protection for Server Workloads



Until now, the best tools organizations have been armed with are “detection and response” solutions that generally discover breaches after they have already occurred. Unfortunately, ransomware attackers have gotten increasingly more sophisticated and aggressive. By the time a breach is detected by EDR products, systems have already been compromised and sensitive data exfiltrated. It is clear that a stronger runtime defense mechanism is required.

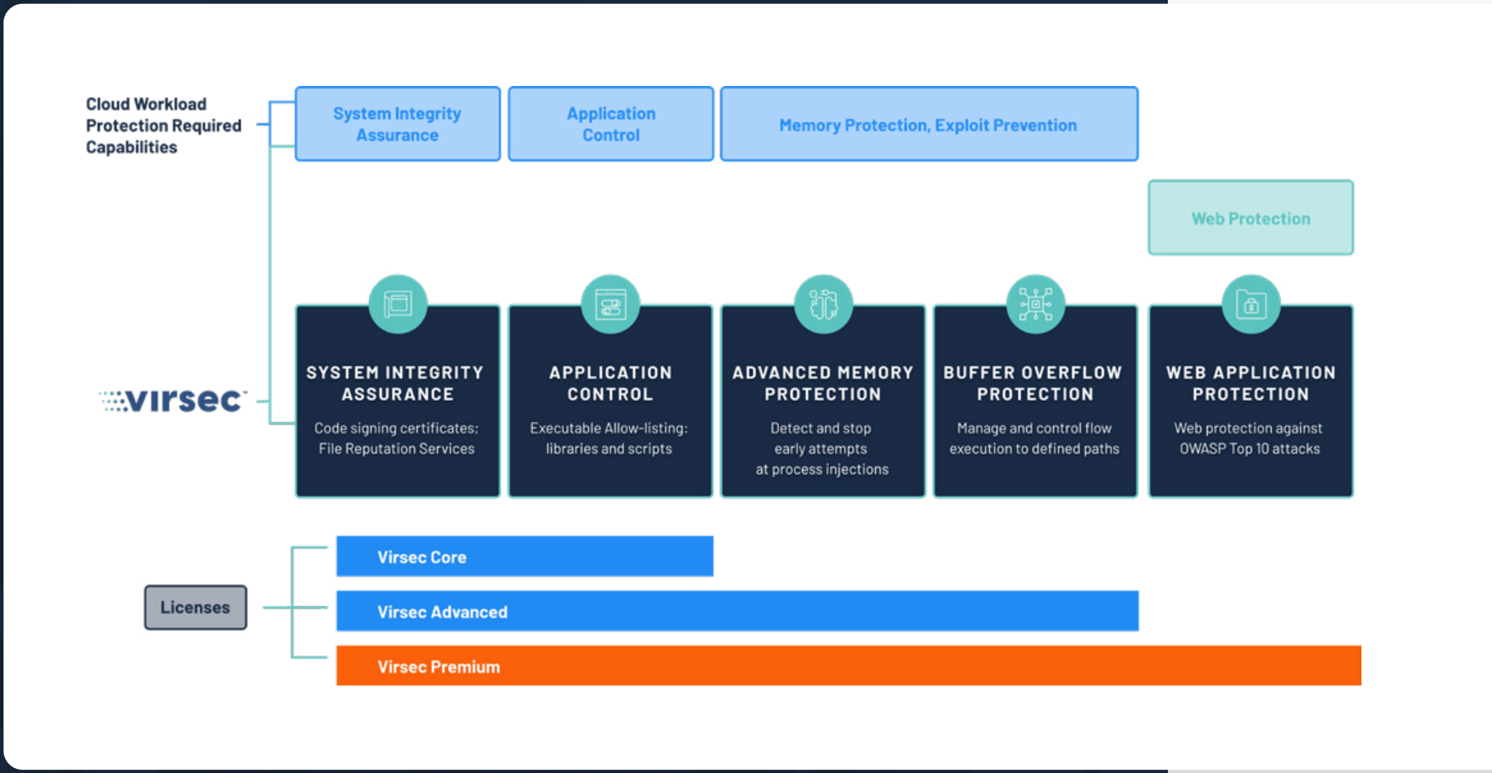
Deterministic Protection

Deterministic protection is a ground-breaking new approach ideally suited for workload security. It relies on automatically mapping what server applications are supposed to do, then stopping any deviations in milliseconds, preventing attackers from leveraging vulnerabilities to take control and run malicious code. A deterministic approach knows exactly what is authorized to run and what should not be allowed to execute. This results in **stopping both known and unknown zero day threats instantly at runtime with very few false positives.**

Virsec Security Platform

Virsec Security Platform (VSP) applies deterministic protection to enable a protection-first strategy. It stops attacks in milliseconds, preventing attackers from leveraging vulnerabilities to take control and run malicious code. VSP is a proven technology that enables leading government and commercial organizations worldwide to protect workloads essential to business at runtime with very high efficacy, thus also drastically reducing false positives.

Virsec proactively **protects against ransomware and malware exploits with VirsecMap**, which defines the executable allow list of what is authorized (system integrity) and **VirsecEnforce which dynamically enforces that the software executes as expected (runtime protection).** With a protection-first approach to zero trust, Virsec 's approach of allowing only 'known good' dependencies such as files, scripts and libraries to run, stops all other malicious behaviors regardless if they are known or unknown attacks. VSP eliminates the logistical nightmare of reacting to vulnerabilities and security patches, and does not require the ongoing update of threat feeds.



Cloud Workload Protection Required Capabilities

System Integrity Assurance

Application Control

Memory Protection, Exploit Prevention

Web Protection

virsec

SYSTEM INTEGRITY ASSURANCE
Code signing certificates; File Reputation Services

APPLICATION CONTROL
Executable Allow-listing: libraries and scripts

ADVANCED MEMORY PROTECTION
Detect and stop early attempts at process injections

BUFFER OVERFLOW PROTECTION
Manage and control flow execution to defined paths

WEB APPLICATION PROTECTION
Web protection against OWASP Top 10 attacks

Licenses

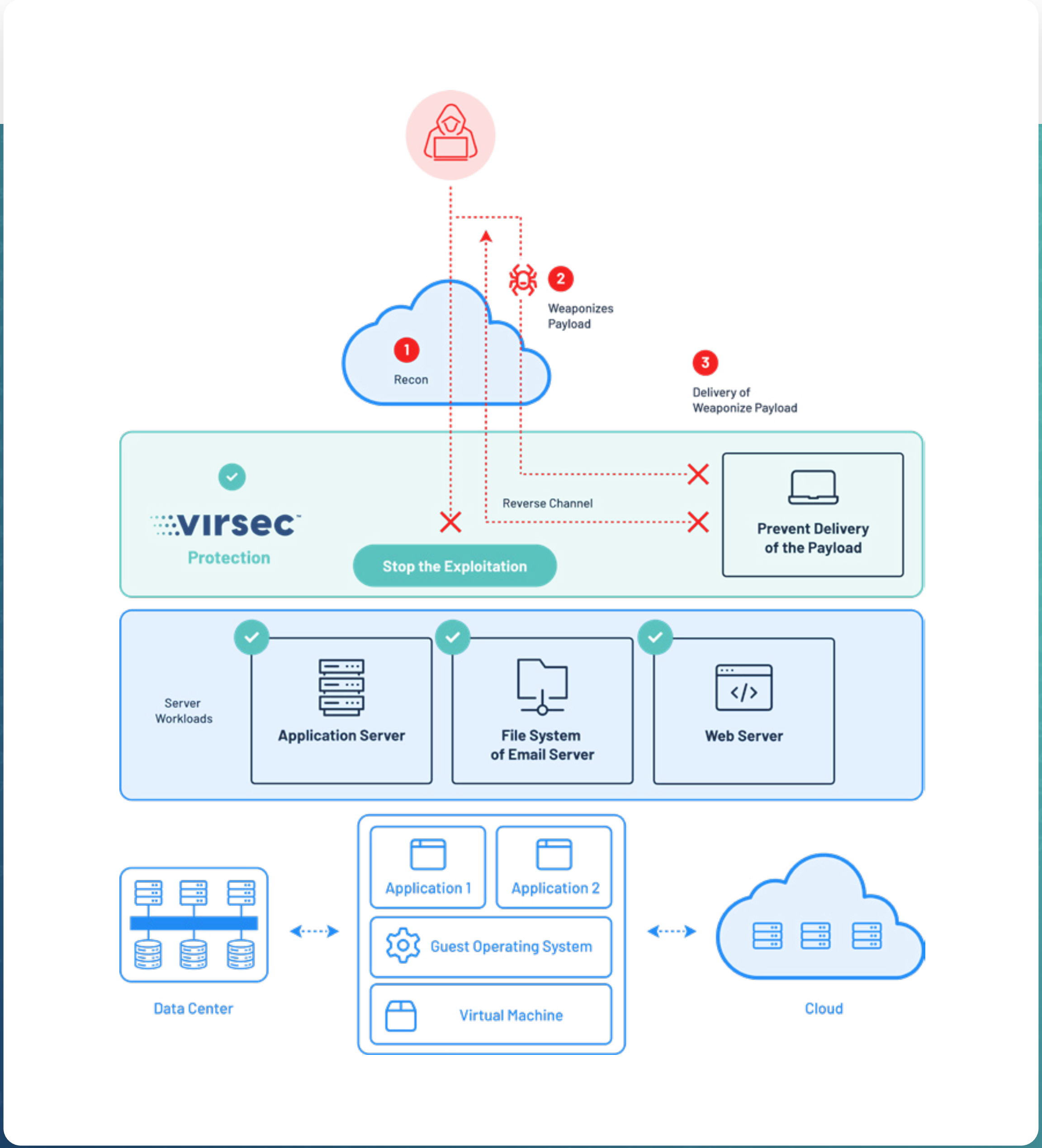
Virsec Core

Virsec Advanced

Virsec Premium

VSP continuously monitors file systems, registry, scripts and processes to ensure system integrity of applications and workloads. It verifies applications are reputable and trusted. This facilitates the automatic detection of DLL injection attacks, and misuse of legitimate software components and tools, without requiring rules and signature updates. Virsec also continuously addresses high-risk and critical Common Vulnerabilities and Exposures (CVEs) and Common Weakness Enumeration (CWEs) and zero-day events without manual efforts or need for expertise, allowing teams to easily deliver on security commitments with less overhead. Furthermore, VSP provides advanced web controls against all OWASP attacks and **deep runtime visibility** into data flowing through your business logic, validating HTTP & SQL input and responses for precise detection.

VSP also prevents lateral progress in the event chain by **blocking unauthorized code execution on host operating systems (OS).**



Conclusion

Ransomware attacks continue to be pervasive and damaging, but there is a solution and end in sight. Public and private organizations are continuing to innovate their thinking and collective need for a new approach to the problem. With government and industry coming together, a portfolio of risk mitigation strategies and offerings, and first-of- a-kind solutions like the Virsec Security Platform that immediately blocks ransomware before damage can be done.

Exploitation Stopped

Endnotes

[1] U.S.-CERT CISA Alert (AA21-243A)

[2] NPR

[3] U.S.-CERT CISA Alert (AA21-243A)

[4] Cybersecurity Ventures

[5] Cost of a Data Breach Report 2021

[6] Cybersecurity Ventures

[7] Sophos

[8] 2021 Data Breach Investigations Report

[9] 2021 Data Breach Investigations Report

[10] Coveware

[11] HelpNet Security

[12] Sophos

[13] Pindrop

[14] Newsweek

[15] The PEW Charitable Trusts

[16] U.S. Government Accountability Office

[17] U.S. Government Accountability Office

[18] Yahoo! Finance

Additional Sources

https://www.washingtonpost.com/politics/2021/09/07/cybersecurity-202-ransomware-is-wreaking-havoc-us-cities/

https://www.policyholderpulse.com/ransomware-insurance-coverage/

https://www.insurancejournal.com/news/national/2021/07/07/621416.htm

https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge

https://www.zdnet.com/article/ransomware-has-become-an-existential-threat-that-means-cyber-insurance-is-about-to-change/

https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/ https://www.cisa.gov/stopransomware