Lessons Learned While Performing 'Hands On' Teaching in a Live Environment

Adamu Yusuf, Justin Clevenger and Char Sample
Marshall University, Huntington, WV, USA

charsample50@gmail.com

Abstract*:* In West Virginia (WV) the county sheriff's office is a central point of interaction between the local government and the people who are served by these elected officials. While law enforcement extends well beyond, this central point of contact, typically the county sheriff website, is not only a great starting point for the citizens to interact with local law enforcement, but also an entry point for potential illegal activities. The county sheriff's offices websites in WV are also the central point for online payment of local taxes, thus making these sites a potential target for electronic misdeeds that would range from defacement to theft and potentially beyond. This study team examined the websites for the 55 counties of WV, in part as a classroom exercise, for potential vulnerabilities ranging from standard server scans to potential exposure through social media (SM) sites where information can be inferred. The majority of SM usage showed professional pages on LinkedIn and Facebook and newer SM sites were not used. The study findings suggest that an overwhelming majority have outsourced services to third party cloud service providers. Overall WV sheriff offices practice good cyber hygiene however, two areas of potential problems are in the duplicate IP addresses found in the cloud service providers shared servers, running multiple services with multiple tenants on the same physical server and the existence of legacy information. The study was neither comprehensive, nor intrusive in nature, but did serve to verify the security posture of the various counties sheriff offices allowing for a fingerprinting of a group of sites in the same industry allowing for a general overall view of security by sector in the public service space. The study also suggested the need for periodic re-checking suggesting a less intense degree, a practice that should be performed regularly in any secure architecture and acts as a public record for interested citizens. A final lesson from the class experience re-iterates the importance of proper scoping.

Keywords: Scans, Tools, Social media, Cloud service providers, Third party, att4ck framework

1. Introduction

Cybersecurity research increasingly focuses on aggregate, posture-based assessments to understand systemic risks and shared vulnerabilities across public-sector organizations, rather than relying solely on incident reporting. ENISA's sectoral threat landscape for public administration highlights that government entities face common threat patterns that can be identified through large-scale, non-intrusive analysis of externally observable infrastructure (European Union Agency for Cybersecurity [ENISA], 2024). ENISA's annual Threat Landscape further emphasizes the value of cross-sector aggregate analysis for identifying emerging threats, shared attack vectors, and trends that go beyond individual organizations (ENISA, 2025). In the United States, CISA similarly promotes proactive cyber hygiene and external attack surface assessments to help state and local governments reduce exposure to vulnerabilities, especially in environments with limited resources and legacy systems (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

The 2025 Marshall University Vulnerability Assessment class was abnormally small and class size afforded the group the opportunity to pick a meaningful target as long as the effort was limited to reconnaissance techniques and the targets were given informed consent, as directed by the Marshall University IRB. Based on this, the sheriff offices for the 55 counties of West Virginia were selected as the target and the letters were sent. The embedded link provides a copy of the letter l Letter Template - justin - char.docx.

2. Background

Research on local governments shows that these entities often face increased cyber risks due to fragmented governance, limited budgets, and dependence on shared infrastructure. This underscores the need for a comprehensive, posture-based evaluation (Hossain et al., 2024). Empirical evidence also suggests that cybersecurity incidents in municipalities have systemic financial consequences; an analysis of over 1,000 cyberattacks against public entities found that municipal borrowing costs increase after publicly reported cyber incidents, reinforcing the broader institutional risks of inadequate cybersecurity posture (Curti et al., 2024).

A recent industry assessment ranked West Virginia among the top states in cybersecurity; however, such evaluations usually focus on reported cyber incidents and state-level malware statistics rather than on proactive assessments of potential entry points within specific government sectors. Prior research has shown that cyber intrusions are often discovered months after the initial compromise, with average detection delays approaching six months, which can obscure underlying vulnerabilities and delay remediation (McDermott, 2025; Total Assure,

2025). Therefore, posture-oriented analyses that examine observable infrastructure characteristics before an incident occurs offer a more forward-looking and insightful perspective on cybersecurity risk.

Public-facing government websites are recognized as essential parts of the public-sector attack surface. Research on government web infrastructure consistently reveals issues like outdated software, exposed services, and weak configurations, which increase the risks of defacement, data theft, and service disruptions (European Union Agency for Cybersecurity [ENISA], 2022). In law enforcement agencies, these risks are even higher because websites act as the main contact points with citizens, including access to public records and online payment systems.

Beyond technical exposure, prior research has emphasized the broader social effects of cybersecurity failures in government systems. Shandler and Gomez (2022), using data from multiple government websites, examined the psychological and social repercussions of cyberattacks on public institutions and found that such incidents can significantly diminish public trust, causing anger, uncertainty, and decreased confidence in affected agencies. While their work focused on results after incidents, it highlights the importance of analyzing government systems as a whole to understand the potential impacts of widespread vulnerabilities.

Several studies have used aggregate methods to analyze government digital environments beyond just incident response. Neumann et al. (2022) examined hundreds of government websites to identify patterns in political communication and public engagement, demonstrating the value of large-scale evaluations of public-sector web presence. The increasing reliance of government agencies on outsourced and cloud-based services highlights the necessity for comprehensive cybersecurity assessments. Sector-level studies have found that shared hosting environments and third-party service providers can pose systemic risks related to multi-tenancy, duplicate IP addresses, and dependence on shared infrastructure components (Bayuk et al., 2018; ENISA, 2022). These risks are especially critical for county-level agencies, where multiple jurisdictions may depend on the same providers, even though they operate independently.

Alongside traditional web and hosting infrastructure, social media platforms have become vital communication tools for law enforcement and other public agencies. While these platforms improve public engagement and facilitate information sharing, overall evaluations of public-sector social media use indicate that these tools are often managed outside formal IT governance frameworks, increasing the risk of data leaks, account breaches, and reputational harm (Cybersecurity and Infrastructure Security Agency [CISA], 2023). Oversight-focused reviews of public organizations also reveal that gaps in governance, risk assessment, and security controls are common across government settings, even when handling sensitive information systems (U.S. Government Accountability Office [GAO], 2017). Despite their operational significance, social media accounts and other visible external assets are frequently excluded from formal cybersecurity posture evaluations.

Although existing literature demonstrates the value of aggregate cybersecurity evaluations in public-sector contexts, limited research has focused specifically on county-level law enforcement agencies or combined analysis of web services, shared hosting dependencies, and social media presence within a single study. This gap motivates the present work, which applies a non-intrusive, properly scoped, aggregate assessment to county sheriff offices in West Virginia. By examining publicly observable infrastructure across a defined sector, this study contributes to a broader understanding of shared cybersecurity practices, common exposure patterns, and overall cybersecurity hygiene in local government environments.

Rather than focus on the aftereffects of failed cybersecurity (Shandler & Gomez, 2022), this study chose a neutral stance on outcomes and was observational in nature. However, findings that would indicate widespread vulnerabilities could predict future breakdowns in the trust between law enforcement and the citizenry or could become a re-enforcement of trust between law enforcement and the population. While this study was not as ambitious as the Shandler & Gomez (2022) study, the cyber aspect with aggregated government data does suggest that this study is of potential interest beyond the confines of West Virginia. The choice of the sheriffs' offices allowed the team to examine a real world, live set of targets while making those targets relatable to the students. The traditional controlled method of using a known site with known vulnerabilities as are used in various cyber exercises provides value to students but is not an accurate reflection of reality and may not provide the best opportunity for students to refine report writing when findings are minimal or even artificially high.

The research question posed was: Using basic reconnaissance techniques, what can be learned about the West Virginia sheriff sites collectively, Or, in other words, is there a collective story to be told about the 55 counties sheriff offices.

3. Method

The data collection phase required a manual search of all 55 counties of WV to determine if the sheriff's office information was available online. All 55 counties had websites that were active. A list was compiled and each site was tested to verify the site was active. Data collection on site data is described later in this section.

The data processing relied on a combination of tools and manual queries. The team was restricted to passive information gathering and the MITRE ATT4CK framework (attack.mitre.org, 2026) enumerate various techniques that are part of the reconnaissance effort. There are 11 techniques listed as part of the reconnaissance phase in assessing vulnerabilities, the team was successful in 5 of the 11 reconnaissance techniques. Table 1: Lists the techniques and provides a status on the attempt and results.

Table 1: MITRE ATT4CK enumeration of techniques and results

Technique	Results & Tool Deployed
Active Scanning	Success, Nmap
Gather victim host information	Success Nmap
Gather victim identity information	Success, Manual searches of social media sites
Gather victim network information	Not successful, no access given and would have required active measures
Gather victim org information	Success, manually accomplished via review of public information
Phishing for information	Not successful, prohibited
Search closed sources	Not successful, limited resources
Search technical databases	Not attempted
Search open websites and domains	Success, domain info via dig, nslookup, other info via Nmap
Search Threat Vendor Data	Not attempted, not available
Search victim owned websites	Not attempted, not available

The team first tested the connectivity of all of the sites ensuring they were up and active. A simple ICMP echo request was performed and a positive response from the site was noted. The lack of a positive response required a traditional web request as some sites block ICMP requests. ICMP requests are faster to evaluate, thus ICMP requests were the preferred initial method of determining connectivity. The **Nmap** scanning tool, while user friendly is time consuming and provides additional information that required additional filtering.

Upon completion of site identification, site gathering domain information followed. The domain information yielded results that gave additional information about the site and what services are outsourced and to whom. The class then invoked the **dig** (Liu et al., 2006) and **nslookup** (Kavieskara, 2021). tools. Students were specifically directed to dig for MX (mail exchange), CNAME (canonical name) for web and other servers, NS (name server) and SOA (start of authority) records in addition to the A records. These records were specifically chosen because they are minimally required for an internet presence and they can provide insight into trusted third parties.

DNS lookups using the **dig** command or the **nslookup** program were performed to gain additional knowledge about the zones. Rather than exploring a group of IP addresses the team examined host names to better understand the nature of the relationships between public hosts in the same domain. Accomplishing this task required more detailed lookups of each of the domains, focusing on specific CNAME, A, MX, NS and SOA records.

The SOA, NS and MX records provided information on the cloud service providers that had been sourced to perform the name service and mail processing. The NS records provided the list of authoritative nameservers for the zone, along with the information on who administers the zone. The MX records point to the host that accepts mail for the zone, once a MX record is retrieved the corresponding A record can give information about the software that accepts the zone's mail.

By gathering the additional information of outsourced sites, the Nmap scans were directed beyond the IP range associated with the webservice and allowed for collection of information about various cloud service providers. While individual DNS queries were time consuming, the information obtained provided insights into sheriff offices and trusted third parties.

All requests and responses were entered into a shared spreadsheet, The initial list of the 55 counties can be found at this link, West Virginia Counties and the shared spreadsheet can be found at Marshall-615.

After the DNS information was captured, port scans were performed on the hosts, and IP address blocks. That results from that scans were put in individual files, and the spreadsheet had the list of IP addresses and open ports for each county. The addresses were sorted and grouped with the intent of finding possible shared spaces, open or unsecured ports and other information.

The final reconnaissance effort was dedicated to social media findings. The social media sites that were probed were Facebook, LinkedIn, Twitter (X) and BlueSky. A test was run comparing the output of popular AI algorithms against the results of manual queries to each of the social media sites. Pilot, ChatGPT, Gemini and Grok were each tried and all of these AI engines were not as accurate as the manual queries.

All results were validated first by the instructor. Nmap scans were run multiple times on targeted IP addresses. Additionally, Nmap queries on ports were manually verified via directly by connecting to the port comparing responses. DNS queries were cross checked with **dig** commands being run on **nslookup** outputs, and **nslookup** commands were run against **dig** commands in each case comparing the outputs.

4. Findings

There were 2 common configurations identified on the web servers, the first was some servers ran on port 80 (HTTP) and performed a hand-off to port 443 (HTTPS), while other servers run strictly on port 443. Furthermore, Furthermore, the HTTPS TLS version number was checked verifying the site is running version is HTTPS v1.2 or v1.3. Both versions are currently acceptable standards (Kohlweiss et al., 2015), although v1.3 is stronger and features forward secrecy.

The social media findings relied on querying the office entity, followed by the sheriff and when available deputy names. Overall, the majority of sites were deemed “safe”, a full 69% (38/55) outsourced the website management to a third-party provider. Outsourcing web and other services to third party providers is quite common and providers are presumed to have financial incentives to enact good cybersecurity practices although evidence of this presumption is lacking. Security varies based on terms of the service level agreements (Nicolazzo et al., 2024). This team did not have access to the service level agreements. What the team did see was some variations in the open ports, although overall the profile was rather consistent across sites. The most consistent configuration showed ports 80 (HTTP) and 443 (HTTPS) as the only open ports on the webserver.

While no specific exploitable vulnerabilities were identified, there were several security irregularities observed. One of the more interesting findings was the 9 cases of shared physical servers (same IP address) with 2 different counties. The cloud service providers business model relies on shared resources, but the exact same IP address for tax payment for WV counties. The team recognized the model of cloud service providers requires the sharing of devices as the cloud model relies on efficiencies where physical devices shared by the customers.

One finding of interest was the failure to fully purge previously owned domain name space. There was a county that when scanned using **Nmap** appeared to have outsourced the DNS service management to a cloud service provider (CSP), however, the **dig** and **nslookup** queries showed a legacy address with the county name but the current address is now affiliated with a business not a sheriff’s office.

Mail Servers The most common e-mail server used was Microsoft Outlook in the Microsoft Cloud (26%). The second most was a cloud service mail solution dedicated for government use (15.2%). Cloud Service Providers (CSPs) collect analytics, in the case of this second group of users, the collected analytics could be grouped with other government entities to reveal potential patterns by targeted sector.

One of the most significant threats to cloud computing is misconfigurations (CSA Working Group, 2024). 9 of the 55 counties shared a mail server with the at least one other West Virginia county. This use of CSPs also suggests a willingness of the counties to employ personnel experienced in core government functions, further investigation could confirm this suggestion.

9/55 counties (16.3%) used the same physical mail server, although not all on the same server. The greatest risk in the cloud environment occurs when cloud tenants self-manage and fail to remain current (Khalil, 2025). Container breakouts are serious, but public facing containers, even when broken are secured to avoid movement into other containers, in part due to isolation of kernel functions (Wu et al., 2020). The top 3 CSP mail solutions were Microsoft Outlook, emailsvr.com and nicusa-gl.com, these 3 sites account for 26 of the 45 active mail sites.

The CSP mail servers ran mail on port 25, showing the port "open" not "filtered". One CSP, not listed above, had additional ports open but filtered, those ports were echo (7), chargen (19) and 22 (ssh).

Of note, 3 counties, were self-managed, these counties security profiles appeared to be slightly less robust than the managed sites, in that the open ports were not filtered. The lack of probing prohibited the group from being able to determine if the "open" ports were running the most up to date fully patched software. One of the self-managed counties showed open ports for DNS (53), HTTP (80), FTP (21) and IMAP over SSL/TLS (993). The self-managed sites did limit the number of open ports on the server.

4.1 Webservers

42/55 (76.36%) counties used HTTP protocols for their tax websites. Of the counties that used HTTPS five used TLSv1.2 & TLSv1.3, two used just TLSv1.2, and two used TLSv1.0, TLSv1.1, and TLSv1.2. No information was able to be obtained from the other four IP addresses.

32 of 55 counties (58%) used the same third-party provider for their web service. There were two primary companies who managed the majority of sites, and both had ports 80 (HTTP) and 443 (HTTPS) open. Minimally port 80 should be filtered, but preferable would be to have all port 80 traffic re-directed to port 443. Considering the site is use for paying taxes the extra privacy granted by using HTTPS instead of HTTP to HTTPS would reduce the risk profile, assuming that they server is well-maintained. One county did not use port 80 and enabled port 443 for web re-direction. Two counties used port 80 exclusively thus potentially exposing private data. The possible status cannot be made any more definite due to the non-probing nature of the study. The possibility does exist that a private session occurs before data is exchanged.

4.2 Social Media

One suggestion that deviates from historic vulnerability analysis deals with the rise of social media usage. Social media presence is considered a part of the current vulnerability assessment process to the extent that social engineering red flags that may allow for attackers to perform traditional attacks like using technical means or social methods where interaction with targets and attackers take place. (Roy et al., 2022) Less effort is spent on using social media for learn more about the target for the purpose of influence operations.

Influence operations when successful can have the target perform the attacker's goals without the attacker needing to take the controls (Tayouri, 2020). Tayouri (2020) noted that influence campaigns can operate outside of the military and political theaters. This type of attack is sometimes referred to as cognitive warfare (Bardin, 2025). The goal in cognitive warfare is to hack the target's thought process.

The process for collecting this information was time-consuming and potential connections or leads were followed (e.g. Sheriff sites that had links to other personnel such as deputies were followed and the deputies were also investigated). Leads could be considered groups associated with the social media site. The team used their personal accounts to explore group memberships on Facebook, Instagram and LinkedIn.

Before examining groups, the team first checked the advertised social media presence of the sheriffs' offices. All of the sites maintained a professional presence without revealing personal preferences. The site messages reflected professional information that aligns with the county websites.

When examined in totality 50 of the 55 counties (90.9%) had a Facebook page. LinkedIn was also a popular choice where 49/55 counties (89.09%) had profiles. The third social media platform was Instagram where 6 of 55 counties (10.90%) had Instagram pages. When determining exposure levels counties with only 1 site presence were considers low exposure, counties with 2 social media sites were considered moderately exposed and those counties with 3 or more sites were considered highly exposed. The exposure has less to do with vulnerabilities than the actual presence where data can be collected and ultimately combined with other data on the targeted person to build profiles. When considered by traditional cybersecurity standards the social media usage by the sheriffs' offices would be considered secure. However, when examined from the perspective of a data scientist where any data exposure has risk, the majority of counties have medium exposure scores. Figure 1 shows the exposure rates for the WV Sheriffs Offices.

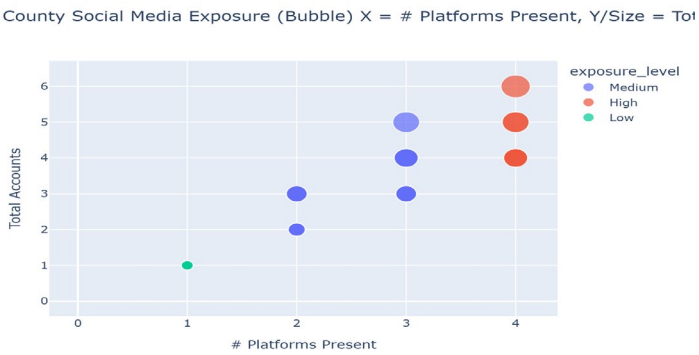

Figure 1: Exposure rates in social media for sheriffs and deputies in WV counties

Other findings: One set of findings that were of interest and ultimately prescient, were outsourcing of name service management to CSPs. Recent outages by AWS (Borngreat-Mensah, 2025) and Cloudflare (Booth, 2025) highlight the vulnerabilities to availability even when CSPs have high availability requirements. The students correctly identified a potential outage by CSP as being a potential risk area, and the recent aforementioned outages provided a real-world example showing the effects of these dependencies. Figure 2 shows the common outsourced services and the usage rate for the providers.

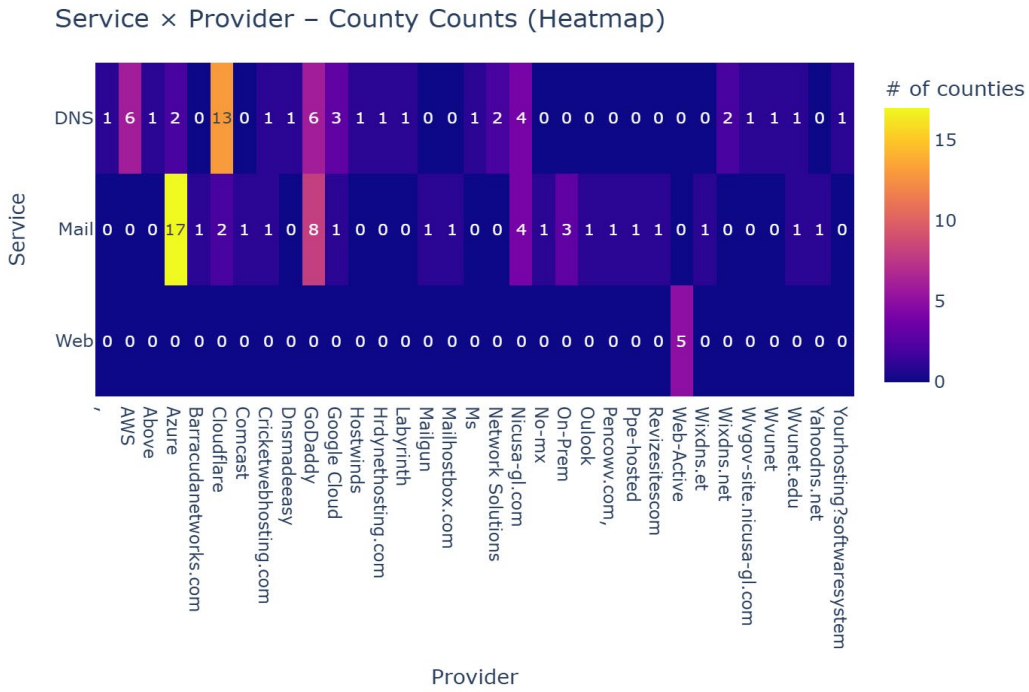

Figure 2: Providers and services, shows the rates of outsourcing critical services and most popular providers

5. Conclusions

This exercise generated a fair amount of enthusiasm at both the institution and within the class while offering a wider aggregated view of the WV Sheriffs offices. The limitations due to equipment and broad scope were difficult to reconcile. The equipment limitation resulted in Nmap scans taking longer than planned. The overall findings largely reflected industry recommendations, limited numbers of open ports and current patched software versions. The most common problems found was the HTTP to HTTPS hand-off issue.

There were individual sites, some self-managed others contractor managed that had a significant number of ports open, that raised concerns. These were not specifically listed in this paper due to privacy concerns and the fact that the county had no agreements in place with the university. These findings while uncommon, serve as outlier to the aggregated data.

The students gained knowledge of underlying technology and methods that are used by scanning tools, thereby giving the students an additional perspective. This exercise in performing non-invasive reconnaissance in a live environment allowed for deeper investigation into the sheriff sites than a basic scan while suggesting potential value in exploring inter-relationships between sites that arise when using the same vendors or cloud service providers.

Several technical recommendations were,

- The clean-up of legacy DNS information. This recommendation is made under the netiquette guidance as well as performance and security concerns.
- Failure to properly maintain or release dated DNS information can lead to slower response times (Zhang et al., 2024), or in some cases DNS hijacking (Ibid). Failure to update DNS glue records is common.
- Follow-up with individual sites that had ports not related to web services open.
- Follow-up with sites that may have potential vulnerabilities identified when compiling this paper.
- Examination of the contractor supply chains through periodic audits should be performed since most sites rely on multiple third-party vendors.

AI statement: This paper was created without the use of Artificial Intelligence (AI) when generating content. AI use was experimental in nature and described in the text of the paper.

Ethics statement: Ethical concerns were addressed at Marshall University where the institutional review board (IRB) determined that due to the non-intrusive nature of the study the IRB process was waived in favor of issuing an informed consent letter to the various counties. The informed consent letter was sent before the study started and a copy of the letter is referenced via an embedded link in the paper.

References

Bardin, J.S., 2025. Cyber warfare. In *Computer and Information Security Handbook* (pp. 1345-1380). Morgan Kaufmann.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2018). *Measuring cybersecurity risk*.

Booth, R. 2025. Cloudflare outage causes error messages across the internet. Retrieved from: https://www.theguardian.com/technology/2025/nov/18/cloudflare-outage-causes-error-messages-across-the-internet

Borngreat-Mensah, P.E.T.E.R., 2025. Mitigating cloud centralization risks: A case study of the October 20, 2025 AWS outage using a multi-cloud dependency mitigation framework (MCDMF). Retrieved from: https://www.researchgate.net/profile/Peter-Borngreat-Mensah/publication/397175468_Mitigating_Cloud_Centralization_Risks_A_Case_Study_of_the_October_2025_AWS_Outage_Using_a_Multi-Cloud_Dependency_Mitigation_Framework_MCDMF/links/6907174f4baee165918f9ccc/Mitigating-Cloud-Centralization-Risks-A-Case-Study-of-the-October-2025-AWS-Outage-Using-a-Multi-Cloud-Dependency-Mitigation-Framework-MCDMF.pdf

Curti, F., Ivanov, I., Macchiavelli, M., & Zimmermann, T. (2024). *City hall has been hacked! The financial costs of lax cybersecurity* [Conference presentation]. Municipal Finance Conference, Brookings Institution. https://www.brookings.edu/articles/what-cyberattacks-do-to-municipal-issuers-borrowing-costs/

Cybersecurity and Infrastructure Security Agency. (2023). *Cyber hygiene services*. Retrieved from:https://www.cisa.gov/cyber-hygiene-services

Cloud Security Alliance, 2024. Top threats to cloud computing. Retrieved from: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024#

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape for the public administration sector*. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Public%20Administration%20TL%202024%20-%20v1.2.pdf

European Union Agency for Cybersecurity. (2025). *ENISA threat landscape*. https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

Hossain, S. T., Yigitcanlar, T., Nguyen, K., and Xu, Y. (2024). *Local government cybersecurity landscape: A systematic review and conceptual framework*. *Applied Sciences, 14*(13), 5501. https://www.mdpi.com/2076-3417/14/13/5501

Kavisekara, H.K.M.U.I.K., 2021. *User Friendly DNS Diagnosing Dashboard* (Doctoral dissertation).

Khalil, M., *The definitive guide to cloud security compliance 2025,* DeepStrike. Retrieved from: https://deepstrike.io//blog/cloud-security-compliance-2025-guide

Kohlweiss, M., Maurer, U., Onete, C., Tackmann, B. and Venturi, D., 2015, November. (De-) constructing TLS 1.3. In *International Conference on Cryptology in India* (pp. 85-102). Cham: Springer International Publishing.

Kornfield, M., 2025. Social Security official says DOGE compromised Americans' data. *The Washington Post*, pp.NA-NA.

Liu, C. and Albitz, P., 2006. *DNS and Bind*. " O'Reilly Media, Inc.".

Madnick, S.E., Li, X. and Choucri, N., 2009. Experiences and Challenges with using CERT Data to Analyzes.

McDermott, J. (2025). Hackers linger for an average of 206 days: Here's how we can spot them on day 1, Retrieved from: https://43tc.com/article/hackers-linger-for-an-average-of-206-days-heres-how-we-can-spot-them-on-day-1/)

McLaughlin, J., (2025). A whistleblower's disclosure details how DOGE may have taken sensitive Labor data. https://www.npr.org/2025/04/15/nx-s1-5355896/doge-nlrb-elon-musk-spacex-security.

MITRE Attack website. Retrieved from http:attack.mitre.org

Neumann, M., Linder, F. and Desmarais, B., 2022. Government websites as data: a methodological pipeline with application to the websites of municipalities in the United States. *Journal of Information Technology & Politics*, *19*(4), pp.411-422.

Nicolazzo, S., Nocera, A. and Pedrycz, W., 2024. Service level agreements and security sla: A comprehensive survey. *arXiv preprint arXiv:2405.00009*.

Roy, S., Sharmin, N., Acosta, J.C., Kiekintveld, C. and Laszka, A., 2022. Survey and taxonomy of adversarial reconnaissance techniques. *ACM Computing Surveys*, *55*(6), pp.1-38.

Srikanth, B., 2022. Ethical Hacking in Network Security: Assessing Vulnerabilities to Improve Defenses.Tayouri, D., 2020. The Secret War of Cyber Influence Operations and How to Identify Them. *Institute for National Security Studies Cyber, Intelligence, and Security Publication*, *4*, pp.5-22.

Total Assure, 2025. Retrieved from (https://www.totalassure.com/blog/average-time-to-detect-cyber-attack-2025,

Townsend, T.C., 1910, August. Taxation Work in West Virginia. In *State and Local Taxation: International Conference under the Auspices of the International Tax Association: Addresses and Proceedings* (Vol. 4, pp. 165-178). National Tax Association.

U.S. Government Accountability Office. (2017). *Federal Student Aid: Better program management and oversight of postsecondary schools needed to protect student information* (GAO-18-121). Retrieved from: https://www.gao.gov/products/gao-18-121

West Virginian News, 2025. Retrieved from: https://www.wvnews.com/news/wvnews/west-virginia-ranks-among-safest-states-for-cybersecurity-in-new-national-study/article_8bcf44a4-ecd5-415a-8ab4-085d95fb00ce.html

Wu, Y., Lei, L., Wang, Y., Sun, K. and Meng, J., 2020, November. Evaluation on the security of commercial cloud container services. In *International Conference on Information Security* (pp. 160-177). Cham: Springer International Publishing.

Zhang, Y., Liu, B., Duan, H., Zhang, M., Li, X., Shi, F., Xu, C. and Alowaisheq, E., 2024. Rethinking the Security Threats of Stale {DNS} Glue Records. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 1261-1277).