Develop a Cybersecurity Infographic

Ryan Coon

CYB-650

Dr. Howard Goodman

August 20, 2025

**Introduction**

The internet has revolutionized global connectivity, dismantling geographical barriers and fostering unprecedented human connection. It simplifies our lives and reshapes the nature of our daily work. The internet also plays a crucial role in maintaining familial bonds, bridging distances between loved ones. However, like any powerful tool, the internet has its drawbacks, necessitating caution and awareness in its usage.

**Internet Use and Risks and IoT**

The internet, a gateway to boundless information and a cornerstone of modern life, presents both incredible opportunities and potential risks. While it's an essential tool, it's crucial to be aware of the dangers of security breaches. Falling victim to online scams can lead to financial loss, data compromise, and even identity theft. Sadly, businesses are also significantly impacted by internet-related risks. Data theft can not only affect the products or services a company provides but also erode the trust of stakeholders and damage the company's reputation over time.

The proliferation of the Internet of Things (IoT) has dramatically expanded the attack surface, introducing novel cybersecurity risks. These interconnected devices, often designed with limited resources for processing and security, become vulnerable gateways for malicious actors. Imagine a vast, sprawling city where every lamppost and mailbox is a potential listening post; this is akin to the risk landscape presented by unsecured IoT devices.



One significant implication is the threat to data protection for intellectual property. As IoT devices collect and transmit vast amounts of data, sensitive proprietary information, trade secrets, and research findings can be exposed(Adeniji & Ifeji, 2023). This data, flowing through the digital ether, is susceptible to interception and theft.

Furthermore, the inherent constraints of many IoT devices, such as limited memory and processing power, often mean that robust security measures are either absent or rudimentary(Befiler, n.d.). This leaves them susceptible to a range of attacks including eavesdropping, spoofing, RF jamming, sybil attacks, sinkhole attacks, and man-in-the-middle attacks, as highlighted in various security reviews(.

Mobile devices, while powerful tools, also represent a critical nexus of risk. They carry our personal and professional lives, making them prime targets for data breaches and unauthorized access. The portability and constant connectivity that make them indispensable also make them vulnerable to physical theft and sophisticated cyberattacks.

A diagram of a security target

AI-generated content may be incorrect.

Over the past two decades, companies have increasingly adopted a new customer acquisition strategy. This involves collecting contact information and analyzing the online behavior of potential customers. This data is often sourced from websites visited by internet users and then sold to marketing firms for profit (Legalnature, n.d.).

As the Internet of Things (IoT) continues to expand and users adopt new devices, the number of associated security threats escalates. Key areas of risk with IoT include:

* Lack of Visibility and Device Management - Difficulty in tracking and controlling connected devices.
* Weak Passwords - The use of easily guessable passwords leaves devices vulnerable.
* Botnets - Networks of compromised devices used to steal data or launch attacks.
* Insecure Data Transfer and Storage - Transmitting or storing data without adequate encryption or protection.

**OWASP and Web Applications**

A web application, or web app, is a software program that operates within a web browser, leveraging cloud services for data transfer. This offers users the convenience of anytime, anywhere access. Users initiate a request from their browser, which is then transmitted over the internet to a web server. The web server, in turn, directs the request to the appropriate destination for the web application (Ring Central, 2025).

Despite the emergence of alternative technologies like mobile and hybrid apps, web applications remain a crucial method for securely connecting to a company's server, especially with the implementation of secure authentication protocols. OWASP (Open Web Application Security Project) is an invaluable resource for bolstering application security against threats and cyberattacks. It helps to reduce system errors and failures, thereby increasing the likelihood of success for the application (VeraCode, 2021).

The OWASP Top Ten provides a standardized awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to a web application(Jones, 2018). The most recent iteration, OWASP Top Ten 2021, highlights key areas of concern that have evolved over time.



According to OWASP, the Top 10 vulnerability risks can be found as the following:

* Broken Access Control - This security vulnerability allows attackers to bypass intended restrictions, enabling them to access, modify, delete, or otherwise manipulate system resources or perform actions that are outside of their authorized permissions. To effectively counter this risk, it is essential to implement rigorous authentication, authorization, and permission checks. These measures ensure that only authenticated and appropriately authorized users are granted access to the system, thereby safeguarding against unauthorized actions.
* Cryptographic Failures - This type of attack exploits vulnerabilities within the Transport Layer Security (TLS) protocol, which is designed to secure communications between clients and servers over networks. Attackers can manipulate the Hypertext Transfer Protocol (HTTP) to create a deceptive experience for the targeted destination. To safeguard against such attacks, it is strongly recommended to utilize the HTTPS protocol for all user-system communications. Additionally, regularly renewing website certifications is a key practice to prevent cryptographic failures.
* Injection - Injection attacks occur when an attacker submits maliciously crafted input, causing the application to perform unintended actions by exploiting syntax errors. To prevent SQL injection attacks, program code should incorporate all syntax within an IF condition statement and properly escape strings containing special characters.
* Insecure Design - This vulnerability arises from flaws in the fundamental design and architecture of a system, leading to numerous threats and vulnerabilities. To mitigate this, programmers must meticulously map the entire data flow of the program, ensuring that no malicious input can exploit gaps to gain unauthorized access. Prevention strategies include a thorough understanding of the system's intended functionality, securing the data flow to account for all potential scenarios, and implementing robust data encryption techniques.
* Security Misconfiguration - Improperly configured system settings are a significant vulnerability, as attackers often exploit default configurations to gain unauthorized access. To prevent attacks stemming from misconfiguration, it is recommended to change all default settings and implement a robust authentication process to secure user access to the system.
* Vulnerable and Outdated Components - This vulnerability arises when a program utilizes third-party libraries, and attackers can exploit flaws within these libraries to compromise the system. Misuse of these components can lead to vulnerabilities such as SQL Injection or Cross-Site Scripting. To mitigate the risks associated with outdated components, it is recommended to automate deployment processes, maintain up-to-date software versions, employ dedicated tools for scanning software code, conduct thorough code reviews, and perform regular penetration testing.
* Identification and Authentication Failures - Password management risks are prevalent, often stemming from employees lacking adequate training on cybersecurity attacks. Furthermore, utilizing social media for authentication is generally unsuitable for company security policies. To prevent password management risks, it is crucial to provide systematic training, educate employees on cybersecurity threats, and prohibit the use of social media authentication for system access. Additionally, implementing strong passwords that incorporate special characters and numbers significantly enhances system security.
* Software and Data Integrity Failures - This risk pertains to code infrastructure that lacks protection against integrity violations, often occurring when a system relies on plugins. These plugins might use libraries to validate code and ensure the system functions correctly. An attacker could potentially upload their own modified version during an update, thereby exploiting the system. To prevent integrity-related risks and failures, it is recommended to ensure plugins are properly updated and that these updates originate from a trusted source.
* Security Logging and Monitoring Failures - Logging is the process where an application records every action performed by the system or its users. Without proper logging, tracking transactions within the system becomes difficult, leaving it vulnerable to various threats. To mitigate the risks associated with logging failures, it is recommended to enable log records on both the server and the user's machine. Furthermore, a robust monitoring process is essential to actively track these logs and address any potential threats as they arise.
* Server-Side Request Forgery (SSRF) - This risk emerges when a server utilizes the HTTP protocol for data transfer, allowing an attacker to initiate HTTP requests originating from the company's web server. To mitigate the dangers associated with server-side requests, it is strongly recommended to adopt the HTTPS protocol, thereby ensuring that the data transfer process is both secure and safe(OWASP, 2021).

**Securing Web Applications**

Developing and implementing strong security for web applications involves a comprehensive strategy that addresses various stages of the application lifecycle. One key area is input validation and sanitization. This involves rigorously checking all data received from users or external sources to ensure it conforms to expected formats and does not contain malicious code(Northwestern University, n.d.). For instance, preventing SQL injection vulnerabilities requires validating user input before it's used in database queries.

Another crucial aspect is authentication and authorization. Implementing strong password policies, multi-factor authentication (MFA), and role-based access control ensures that only legitimate users can access the system and that they have the appropriate permissions. As highlighted by OWASP, "Authentication and Session Management" is a critical area to address(OWASP, 2017).

Secure coding practices are fundamental. Developers should be trained on secure coding principles, such as avoiding hardcoded credentials, properly handling errors, and preventing cross-site scripting (XSS) vulnerabilities. Following guidelines like the OWASP Top 10 provides a roadmap for addressing the most critical web application security risks.

Regular security testing is indispensable. This includes penetration testing, vulnerability scanning, and code reviews. Tools can help identify weaknesses, but manual testing and expert review are often necessary to uncover complex vulnerabilities. Automated deployment processes can also help ensure that security patches are applied promptly.

Web Application Firewalls (WAFs) play a vital role in real-time protection. WAFs can filter, monitor, and block malicious HTTP traffic to and from a web application, helping to mitigate threats like SQL injection and cross-site scripting. Implementing in-line security controls such as rate limiting and sensitive data masking further strengthens defenses.

Keeping software up-to-date is also paramount. This includes the application itself, as well as all libraries, frameworks, and server software. Vulnerable and outdated components are frequently exploited by attackers. Regularly scanning software code and performing code reviews can help identify and address these risks.

Finally, security logging and monitoring are essential for detecting and responding to security incidents. Comprehensive logging of system and user activities allows for the tracking of transactions and the identification of suspicious behavior(Williams et al, 2022). A proactive monitoring process can help close potential threats before they escalate.

References:

Adeniji, Oluwatoyin, and Chinaza Ifeji. *Privacy Implications of IoT: Data Protection and Consent in a Connected World*. 14 Dec. 2023, www.researchgate.net/publication/376503266\_Privacy\_Implications\_of\_IoT\_Data\_Protection\_and\_Consent\_in\_a\_Connected\_World.

Boeckl, Katie, et al. “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.” *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, June 2019, nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf, https://doi.org/10.6028/nist.ir.8228.

Buntz, Brian. “10 IoT Security Targets.” *Iotworldtoday.com*, 2016, www.iotworldtoday.com/security/the-10-most-vulnerable-iot-security-targets.

Hassen Hannachi. “Definition the Open Worldwide Application Security Project (OWASP) Is a Nonprofit Foundation Dedicated to Improving Software Security. It Operates under an “Open Community” Model, Which Means That Anyone Can Participate in and Contribute to OWASP-Related Online Chats, Projects, and More.” *Linkedin.com*, 19 Feb. 2024, www.linkedin.com/pulse/owasp-top-10-understanding-most-critical-application-risks-hannachi-ykmde.

Jones, Jedd. “11 Best Practices for Developing Secure Web Applications.” *Lrswebsolutions.com*, LRS Web Solutions, 17 May 2018, www.lrswebsolutions.com/Blog/Posts/32/Website-Security/11-Best-Practices-for-Developing-Secure-Web-Applications/blog-post. Accessed 20 Aug. 2025.

LegalNature. “Why You Need a Website Terms of Use Agreement | LegalNature.” *Www.legalnature.com*, www.legalnature.com/guides/why-your-website-needs-a-strong-terms-of-use-agreement-and-what-to-include.

Ltd, Befiler (Pvt). “Intellectual Property: Interesting and Relevant Things to Know About.” *Befiler*, www.befiler.com/blog/intellectual-property-interesting-and-relevant-things-to-know-about.

Northwestern University. “Guide to Securing Web Applications: Information Technology - Northwestern University.” *Www.it.northwestern.edu*, www.it.northwestern.edu/about/policies/webapps.html.

OWASP. “Application Security Risks | OWASP.” *Owasp.org*, owasp.org/www-project-top-ten/2017/Application\_Security\_Risks.

OWASP. “OWASP Top Ten Web Application Security Risks | OWASP.” *Owasp.org*, owasp.org/www-project-top-ten.

Pinto, George P, et al. “A Systematic Review on Privacy-Aware IoT Personal Data Stores.” *Sensors*, vol. 24, no. 7, 29 Mar. 2024, pp. 2197–2197, www.ncbi.nlm.nih.gov/pmc/articles/PMC11014407/, https://doi.org/10.3390/s24072197.

Ring Central. “RingCentral Unified Communications Reference Architecture.” *Ringcentral.com*, 2025, partnersupport.ringcentral.com/network-and-system-requirements/network-requirements/overview/ringcentral-unified-communications-reference-architecture.html. Accessed 20 Aug. 2025.

Veracode. “OWASP Top 10 Vulnerabilities.” *Veracode*, 2021. www.veracode.com/security/owasp-top-10.

Williams, Phillip, et al. “A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies.” *Internet of Things*, vol. 19, no. 100564, July 2022, p. 100564, www.sciencedirect.com/science/article/pii/S2542660522000592, https://doi.org/10.1016/j.iot.2022.100564.