Cybersecurity at TravelNet Solutions

NEXT 2025

The **Heart** of Hospitality

Why do Cyber Attacks Happen to Businesses?

- Financial Gain
  - Cybercriminals may target businesses to steal sensitive financial information, such as credit card details of guests or hosts. This stolen data can be sold on the dark web or used for fraudulent activities
- Sensitive Information
  - Personal and financial information about guests and hosts. Cybercriminals may attempt to breach systems to obtain this data for identity theft, blackmail, or other malicious purposes
- Ransom and Extortion
  - Cybercriminals can deploy ransomware to encrypt critical data on the Airbnb platform, demanding a ransom from the business in exchange for the decryption key
- Competitive Advantage
  - Competitors or individuals with malicious intent may target businesses to gain a competitive advantage or steal confidential information or sabotage the business's reputation
- Bragging rights

NEXT 2025

Cybersecurity Mission

To safeguard our organization's digital assets through proactive risk assessment and robust security measures

- **Prevent**
  - Use tools and practices to prevent cyber attacks
- **Govern**
  - Develop a strong cybersecurity culture
  - Policies, procedures, and practices to manage and protect digital assets from cyber threats
- **Identify**
  - Identify assets and associated security risks
- **Protect**
  - Implement controls to manage security risks
- **Detect**
  - Detect and analyze cybersecurity events to identify cybersecurity incidents

Cybersecurity Program

- **Confidentiality** - Keeping sensitive information private and accessible only to authorized individuals
- **Integrity** - Maintaining data accuracy and guarding against unauthorized changes
- **Availability** - Ensuring systems and data are accessible when needed
- **Authentication** - Verifying user or system identities
- **Authorization** - Controlling access based on permissions
- **Data Encryption** - Protecting data through coding and infrastructure
- **Intrusion Detection & Prevention** - Identifying and blocking unauthorized access
- **Vulnerability Management** - Updating systems to fix vulnerabilities
- **Vulnerability Assessment** - Finding and addressing weaknesses
- **Incident Response** - Managing the impact of security incidents
- **Firewalls** - Filtering application and network traffic
- **Malware Protection** - Defending against malicious software
- **Security Awareness Training** - Educating users on best practices
- **Data Backup & Recovery** - Restoring information in case of loss
- **Secure Software Development** - Embedding security in the software lifecycle
- **Cloud Security** - Protecting data and applications in cloud environments
- **Regulatory Compliance** - Meeting legal and industry requirements

NEXT 2025

Cybersecurity Frameworks and Controls

- NIST (National Institute of Standards and Technology)
- CIS (Center for Internet Security)
- AWS Foundation Security
- PCI DSS (4.0)

NIST Framework Overview

- **CSF Core**
  - The nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.
- **CSF Organizational Profiles**
  - Mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- **CSF Tiers**
  - Can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

Note: CSF stands for Cybersecurity Framework

NIST Framework Overview

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

NEXT 2025

CIS Controls Overview

- The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture. Today, thousands of cybersecurity practitioners from around the world use the CIS Controls and/or contribute to their development via a community consensus process.

CIS Controls Overview

CIS Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

CIS Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

CIS Control 4: Secure Configuration of Enterprise Assets and Software

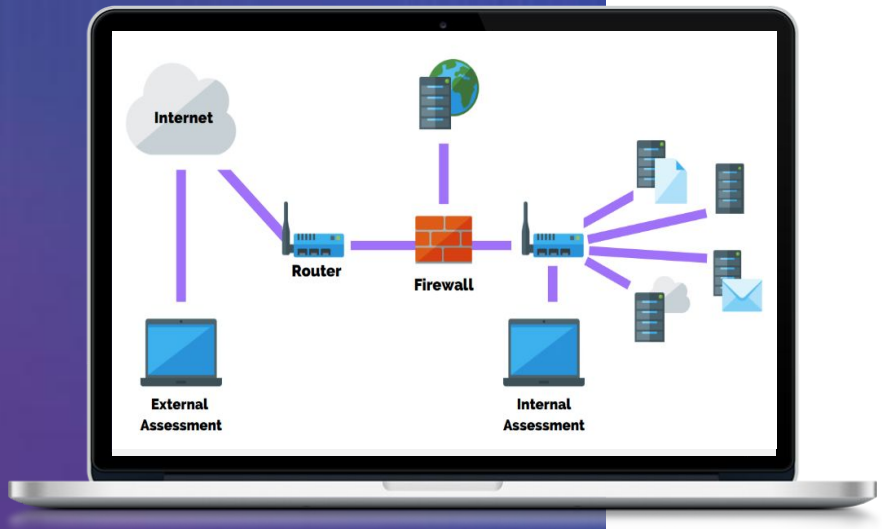
Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Defense in Depth

- Strategy where multiple layers of security measures are implemented to protect an organization's data and systems, essentially creating a multi-layered defense against cyber threats
  - **Security awareness training: Educating employees about cybersecurity policies and best practices**
  - **Phishing Campaigns across the company**
  - Network security: Firewalls, intrusion detection/prevention systems (IDS/IPS)
  - Endpoint security: Antivirus software, endpoint detection and response (EDR/XDR)
  - Application security: Secure coding practices, vulnerability scanning (SAST/DAST)
  - User access control: Strong passwords, multi-factor authentication (MFA), Single Sign-on (SSO)
  - Data encryption: Encrypting sensitive data at rest and in transit
  -

NEXT 2025

Cybersecurity Assessments



- Benchmarking Tools based on NIST, CIS, AWS frameworks
  - Cloud security posture
- Penetration Testing (Third-party firm)
  - Whitebox
    - Tester has knowledge of the environment
  - Blackbox
    - Tester has no knowledge about the environment
  - Internal & External Network
- User access reviews across the enterprise and hosting environments
- Vendor reviews (SOC, PCI, Security questions)

NEXT 2025

Enterprise Security Services

AREA 1 SECURITY

Email Security

- Globally distributed sensors
- Comprehensive attack analytics
- Proactively identifies phishing campaigns
- Preemptive action against targeted phishing, including malware, spoofing attacks

SentinelOne (EDR + XDR)

- Endpoint Detection & Response (EDR)
- Extended Detection and Response (XDR)
- Threat intelligence with AI and machine learning
- Deep learning algorithms

DNSFilter

DNSFilter (DNS Protection)

- Malicious domain protection
- Remote protection
- Website categorization
- Universal domains lists
- AppAware
  - Automatically block risky applications

Enterprise Security

Uptycs
Vulnerability Scanning

- Vulnerability management
- Agent scans
- Unified detections across the enterprise
- Operation reports

Securonix
SIEM

- Security Information and Event Management (SIEM)
- Unified threat detection with AI
- Investigations
- Alerting and Response

Atera
Configuration Management

- Configuration Management
- System Monitoring
- Patch Management
- Software Management
- Remote Access Management
- Network security scans

NEXT 2025

Enterprise Security

1Password
Password Manager

- Password and Key Vault
- Secure credentials sharing
- Monitoring Password health and Breach Insights

GAT+
Audit Tool

- Auditing of user accounts, login locations, email, Google Drives, and browsers
- Risk Assessment of applications
- Monitoring and alerting
- Permission Management

NINJIO
Security Awareness Training

- Secure Coding
- Password and Key storage
- Latest threats
- Malware
- Phishing, Vishing
- Social Engineering
- PCI
- GDPR, CCPA

Hosting Security

AWS SSO & Google Workspace

- Single-Sign On Access to all AWS Services and Infrastructure
- Google Workspace as IDP

AWS Security Lake with AWS OpenSearch

- Centralized security logs aggregation
- Security analytics with AWS OpenSearch service
- Enhanced threat hunting
- Real-time security monitoring and alerting

wazuh.

Wazuh (XDR)

- Extended Detection and Response (XDR)
- Threat hunting
- Vulnerability detection
- File integrity monitoring (FIM) with OSSEC
- Malware detection

NEXT 2025

Hosting Security

AWS WAF Firewall

- Web traffic filtering
- Monitor, block, or rate-limit common and pervasive bots
- Traffic visibility and metrics
- Up to date IP Black lists
- Managed rules from multiple vendors (AWS, Fortinet, F5)
- Custom rules

AWS Network Firewall

- Intrusion Prevention System (IPS)
- Real-time network and application layer protections (exploits and brute force attacks)
- Managed rules from multiple vendors (AWS, Fortinet, F5)

AWS GuardDuty

- Intrusion Detection System (IDS)
- Account level threat detection
- Continuous monitoring across AWS accounts and workloads
- Threat detection, response and remediation
- Malware protection

Hosting Security

Aikido
Vulnerability Scanning

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Cloud posture management (CSPM)
- Open source dependency (SCA). SBOMS, Libraries

Clone Systems
Vulnerability Scanning

- Website, Network and operating system vulnerability scanning
- Automated scripted Pentest
- Infrastructure vulnerability assessment
- PCI compliance scanning

AWS Security Hub

- Cloud Security Posture Management (CSPM)
- Continuous monitoring of security configurations based on the latest benchmarks
- NIST, CIS, and AWS security frameworks

Security Operations Center (SOC)

- 24/7 Monitoring and Alerting
- Monitoring of Employee laptops
- Monitoring of all security events across the enterprise
- Monitoring of the network for potential threats
- Reporting of critical vulnerabilities

NEXT 2025

Vulnerability Management Program

Discovery

- A process for checking all an organization's IT assets for known and potential vulnerabilities
- Vulnerability scanning
- Penetration Testing

Categorization and Prioritization

- Once vulnerabilities are identified, they're categorized by type (for example, device misconfigurations, encryption issues, sensitive data exposures) and prioritized by level of criticality

Resolution

- Remediation- Fully addressing a vulnerability so it can no longer be exploited
- Mitigation - Making a vulnerability more difficult to exploit and lessening the impact of exploitation without removing the vulnerability entirely.
- Acceptance - Leave a vulnerability unaddressed. Vulnerabilities with low criticality scores, which are unlikely to be exploited or unlikely to cause significant damage, are often accepted

Reassessment

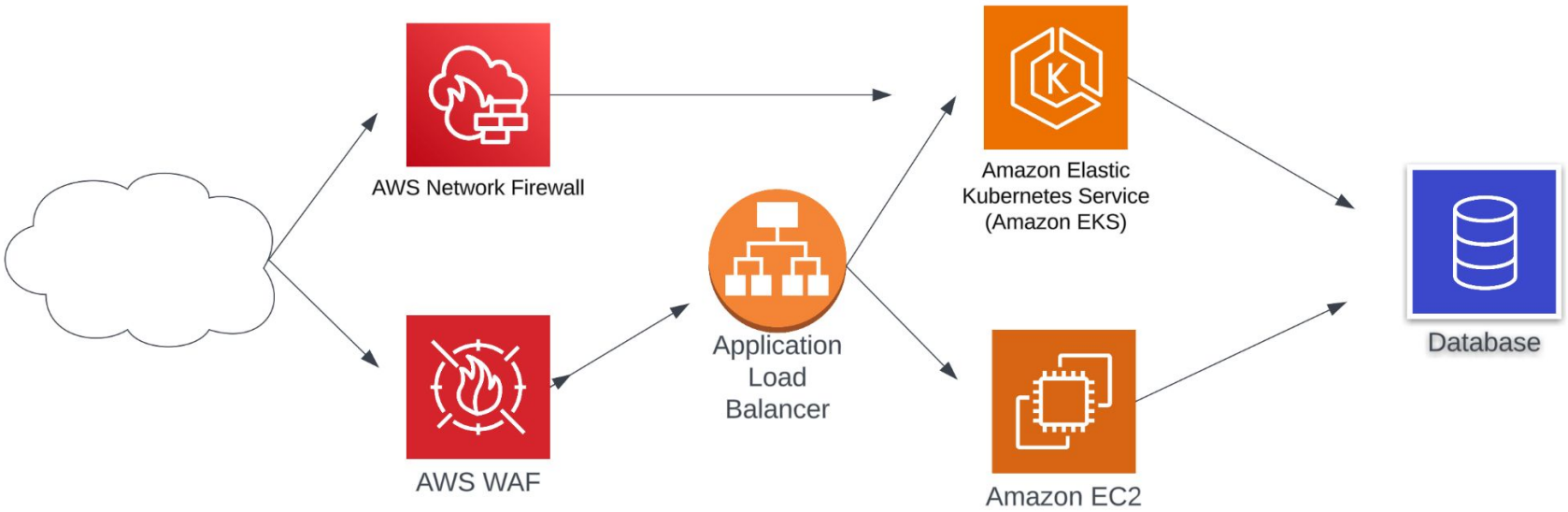
- Conduct a new vulnerability assessment to ensure that their mitigation or remediation efforts worked

Reporting

- Track the resolution of identified vulnerabilities
- Report on metrics like mean time to detect (MTTD) and mean time to respond (MTTR)

NEXT 2025

WAF and Network Firewalls



Common Cybersecurity Threats Impacting the Vacation Rental Industry

- Phishing Attacks
  - Emails, text messages, phone calls
- Social engineering
  - Gather information about the company and infrastructure
  - Credentials & Identity theft
  - Sabotage a business's reputation
- Spoofing/ Fake listings
  - Fake property listings, stolen photos, tricking people into booking a fake property
- Credit Card testing
  - Threat actors get access to credit card numbers (acquired through the dark web) and test them against the website to check to see if the card numbers are valid
- Man-in-the-Middle (MitM) Attack
  - In a MitM attack, an attacker intercepts communication between two parties to eavesdrop, steal information, or alter the communication without either party's knowledge.
- Ransomware (Malicious software to encrypt critical data and demand a ransom)

NEXT 2025

Common Cybersecurity Threats Impacting the Vacation Rental Industry

- Attacks come in waves in the VR industry. We see heavy activity during the holidays (Oct, Nov, Dec)
  - Generally attacks are spread out through the year
- Code Injection Attacks
  - Malicious attack where a hacker exploits vulnerabilities in an application to insert and execute their own arbitrary code within the system
  - SQL Injection Attacks - Exploit vulnerabilities in application and inject database code, access to sensitive data
  - Cross-site scripting (XSS) inject malicious code (typically JavaScript) into a trusted website, enabling them to execute unauthorized actions on a victim user's browser
- Password Attacks
  - Involve various methods to guess or crack passwords, such as brute force attacks, where attackers try all possible combinations, or dictionary attacks, where they use common words or phrases
- Insider Threats
  - Involve individuals with authorized access to a system or network who misuse their privileges to steal data, cause damage, or carry out malicious activities
- AI-Powered Attacks
  - Using AI and Machine Learning algorithms to identify vulnerabilities, deploy campaigns along identified attack vectors, advancing attack paths, establishing backdoors within systems, exfiltrating or tampering with data, and interfering with system operations
- Denial-of-Service (DoS) Attacks

NEXT 2025

How to Recognize Phishing Emails

From: <support@tnsincs.com> The expected From address is support@tnsinc.com, but this email is from support@tnsincs.com
Date: Wed, Sep 18, 2024 at 8:35 AM
Subject: Account Verification Required - Ref: J792IS3414
To: J992IF1413 http://propertyrentals.trackhs.com/ <John@propertyrentals.rentals>

Dear Manager,

We are writing to notify you of significant security enhancements implemented on our platform. Considering these upgrades, we kindly request that all users reconfirm their accounts to uphold the safety and security of our platform.

Please confirm your account by clicking the link below.

Confirm account: https://tnsinc.com/account

Please take note that failure to reconfirm your account within the next 24 hours may necessitate a temporary suspension of your account. This measure is essential to verify your identity and ensure the integrity of your account. We prioritize the security of our valued users, and these actions are undertaken with your protection and the community's well-being in mind. If you have any inquiries or concerns regarding this procedure, please do not hesitate to reach out to our customer support team at https://tnsinc.com/contact/ We appreciate your collaboration in our collective efforts to maintain a secure and safe community.

Warm regards,
Security Team at TravelNet Solutions

NEXT 2025

How to Recognize Phishing Emails

From: <support@tnsincs.com>
Date: Wed, Sep 18, 2024 at 8:35 AM
Subject: Account Verification Required - Ref: J792IS3414
To: J992IF1413 http://propertyrentals.trackhs.com/ <John@propertyrentals.rentals>

Dear Manager,

We are writing to notify you of significant security enhancements implemented on our platform. In light of these upgrades, we kindly request that all users reconfirm their accounts to uphold the safety and security of our platform.

Please confirm your account by clicking the link below.

Confirm account: https://tnsinc.com/account

Please take note that failure t ithin the next 24 hours may necessitate a temporary suspension of your account. This measure is essential to verify e integrity of your account. We prioritize the security of our valued users, and these actions are undertaken with y munity's well-being in mind. If you have any inquiries or concerns regarding this procedure, please do not hesitate to reach out to our customer support team at https://tnsinc.com/contact/ We appreciate your collaboration in our collective efforts to maintain a secure and safe community.

https://
propertyrentals.tnsincs.com/
propertyrentals/

Warm regards,
Security Team at TravelNet Solutions

NEXT 2025

How to Recognize Phishing Emails

From: <support@tnsincs.com>
Date: Wed, Sep 18, 2024 at 8:35 AM
Subject: Account Verification Required - Ref: J792IS3414
To: J992IF1413 http://propertyrentals.trackhs.com/ <John@propertyrentals.rentals>

Dear Manager,

We are writing to notify you of significant security enhancements implemented on our platform. In light of these upgrades, we kindly request that all users reconfirm their accounts to uphold the safety and security of our platform.

Please confirm your account by clicking the link below.

Confirm account: https://tnsinc.com/account

Please take note that failure to reconfirm your account within the next 24 hours may necessitate a temporary suspension of your account. This measure is essential to verify your identity and ensure the integrity of your account. We prioritize the security of our valued users, and these actions are undertaken with your protection and the community's well-being in mind. If you have any inquiries or concerns regarding this procedure, please do not hesitate to reach out to our customer support team at https://tnsinc.com/contact/ We appreciate your collaboration in our collective efforts to maintain a secure and safe community.

https://
propertyrentals.tnsincs.com/
propertyrentals/

Warm regards,
Security Team at TravelNet Solutions

NEXT 2025

How to Recognize Phishing Emails

- Check the email domain
- Look for misspelled domains
  - Threat actors often register domain names that closely resemble legitimate ones
- Poorly written content
  - Phishing emails are often poorly written, with grammar and spelling mistakes. Many scammers come from non-English-speaking backgrounds, leading to unusual or incorrect phrasing
- Urgency or pressure
  - Be cautious of emails that create a sense of urgency, such as "Please act within 24 hours," or that include multiple hyperlinks asking for sensitive information, such as account details or credentials
- Check hyperlinks
  - If the email contains links, hover over them without clicking to reveal the actual destination address. If it doesn’t match what you expect, it’s likely a phishing attempt
- Use an email investigation tool: For further investigation, you can use tools like MXToolbox to analyze the email header
- Email Protection service
  - Ensure that all of your company emails are being scanned and protected by Email Protection services (Examples of such services: Area 1, Trustifi, Mimecast, Barracuda). Add a block rules to block malicious domains

NEXT 2025

Strengthen your Cybersecurity Posture

Cybersecurity Culture

- Security & Acceptable Use Policies
- Security Awareness Training across the company
- Continuous security training for the security team
- Incident Response Plan (IRP)
- Conduct a Security Tabletop Exercise
  - Simulate a real world cybersecurity incident
  - Assign roles to participants (Example: Finance, Legal, Support, Infrastructure, Developer)
  - Discuss the IRP
  - Identify gaps and remediate
- Conduct Phishing Campaigns (KnowBe4, ProofPoint)
  - Send simulated phishing emails to all employees
  - Provide training to employees, who click on the malicious links
- Report spam emails and anomalies to IT (If you see something, say something)
- Encrypt emails with sensitive information
- Use unique accounts, limit account sharing
- Performing background checks on employees for past cyber criminal history

NEXT 2025

Strengthen your Cybersecurity Posture

Technology

- Endpoint protection (EDR)
  - Malware protection
- Aggregate and monitor logs (Managed Detection and Response (MDR)/SIEM)
- Email protection service
- Centralize your user accounts (Example: Google Workspace, Active Directory, Azure AD)
- Use 14+ character passwords with complexity
- Implement Single Sign-on authentication or MFA authentication
- Password vault to store credentials and keys
- User Access - Principle of least privilege, role-based access
- Zero Trust Models for remote access (Example: Teleport)
- Use VPN when using public wifi
  - Wireguard, OpenVPN
- Encrypt data (In flight and at rest)
  - Encrypt laptop drives, application server storage, file storage, and database storage
- Ensure users are using approved applications on company owned systems
- Implement a File Integrity Monitoring tool to monitor and alert for file changes

NEXT 2025

Strengthen your Cybersecurity Posture

Technology

- Vulnerability Management
  - Vulnerability scans and penetration testing
  - Keep vulnerabilities down (Address critical vulnerabilities as fast as possible)
  - Ensure all systems (Laptops, servers, websites, applications, database applications) are patched
- Ensure users are using approved applications on company owned systems
- Protect Websites and other application endpoints with WAF and Network Firewalls
  - Bots
  - Black lists
  - Cross-site scripting (XSS)
  - Distributed Denial-of-Service (DDoS) Attack
- Implement an IDS/IPS
- Backup data regularly and conduct regular backup tests
- Disaster Recovery Plan and Processes
- Limit Access to Systems (Principle of least privilege)
  - Employees only have the necessary access to do their jobs
- Implement the most secure security protocols and algorithms
  - TLS 1.2, TLS 1.3
  - AES, RSA, Triple DES with 256 bit or larger encryption key

NEXT 2025

Strengthen your Cybersecurity Posture

Technology

- Use reCaptcha or hCaptcha for your websites
  - Challenges to distinguish between human users and automated scripts
  - reCAPTCHA v3 uses advanced risk analysis to assess user behavior, while hCaptcha only needs to be integrated on pages you want to protect
- Limit access to the service account or roles used by the application to access backend services
  - Example: No Administrator level access
- Add Implement Content Security Policy (CSP) and other security headers to your website
  - Content-Security-Policy header allows you to restrict which resources (such as JavaScript, CSS, Images, etc.) can be loaded, and the URLs that they can be loaded from
- Scan websites for any changes
- Keep all plugins, themes, and libraries up to date
- Log all website activity to a central logging service
- Store secure keys in a vault
  - Applications can use role based authentication to access the key to prevent keys from being stored in the application configuration

NEXT 2025

Hacking Statistics

- **88%** of cybersecurity breaches are caused by human error. (Stanford)
- The average time to identify a breach is **194** days. (IBM)
- The average lifecycle of a breach is **292** days from identification to containment. (IBM)
- Over **560 million** Ticketmaster customers had their information stolen in a 2024 breach. (BBC)
- In 2023 T-Mobile disclosed its second data breach of the year involving the theft of **836** customers' personal data, the first data breach affected approximately **37 million** customers. (itgovernanace)
- In 2023, X (formerly Twitter) was targeted by a criminal hacker that leaked more than **220 million** users email addresses. (IT Governance)
- In 2023 AT&T a breach exposed approximately **9 million** customers' personal details. (IT Governance)
- A 2021 LinkedIn data breach exposed the personal information of **700 million** users or about **93** percent of all LinkedIn members. (RestorePrivacy)
- A 2020 Twitter breach targeted **130** accounts including those of past U.S. presidents and Tesla CEO Elon Musk, resulting in attackers swindling $121,000 in Bitcoin through nearly 300 transactions. (CNBC)

NEXT 2025

Online Resources

- NIST Controls
  - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- CIS Controls
  - https://www.cisecurity.org/controls
- CISA Threat and Advisories
  - https://www.cisa.gov/topics/cyber-threats-and-advisories
- SecurityWeek
  - https://www.securityweek.com/
- SentinelOne Security Trends
  - https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/
- Google Threat Intelligence
  - https://cloud.google.com/blog/topics/threat-intelligence/
- Splunk
  - https://www.splunk.com/en_us/blog/learn/cybersecurity-trends.html

NEXT 2025

NEXT 2025


The Heart of Hospitality