Why IT Directors Should Care About Web Security

Tech Forward 2025

TECHIMPACT®
Digital Services Division

Hi there!

Marcus Iannozzi

Chief Digital Officer at Tech Impact

He/Him/His

How about you?

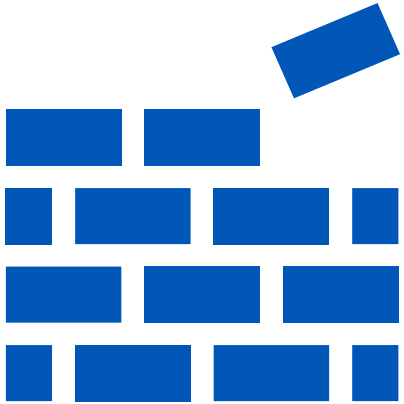
How many folks in the audience…

- Are IT professionals? Web / Comms Staff? Leadership?
- Specialize in cybersecurity within your organization?
- Don’t include your website in security practices?
- Include your site but don’t have the full picture?
- Have more than one staff member managing your website?

Websites are a critical piece of your technology infrastructure.

From Marketing to Mission-Critical

- Perception Issues
- Resource Constraints
- Organizational Silos
- Technology Complexity
- Competing Priorities



Need: Shift Perspectives from Marketing to Infrastructure that Stores Trust

Stakes are High

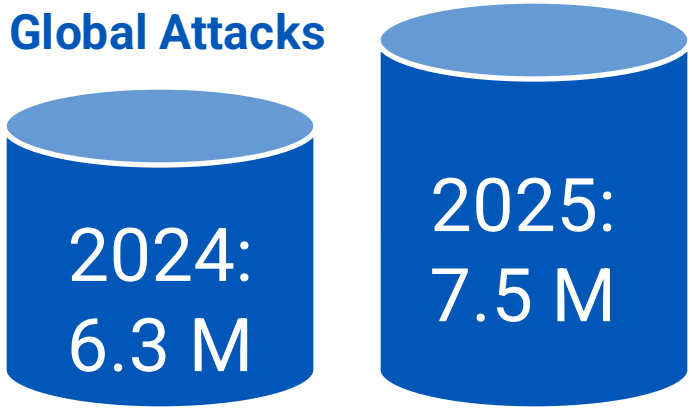
- Damage Trust, Reputation, Mission
- Operational / Communications Disruption
- Financial Losses and Legal Liability
- Integrations and Dependencies
- Potential to Impact Most Vulnerable

Incidence

Nonprofit Sector

1. 1,636 cyberattacks / week, or 58,896 this year
2. 27% of nonprofits have experienced at least one attack
3. Human rights and civil society nonprofits saw 241% increase in DDoS attacks from 2024 to 2025
4. Nonprofits are 2nd most-targeted sector by nation-state actors

Global Attacks



Sources:
https://www.demandsage.com/cybersecurity-statistics/
https://tardigradetechnology.com/blog/key-nonprofit-cybersecurity-statistics-2025/
https://nethope.org/toolkits/2025-state-of-humanitarian-and-development-cybersecurity-report/

Incidents

Web- and Cloud-Based high-profile incidents in nonprofit sector

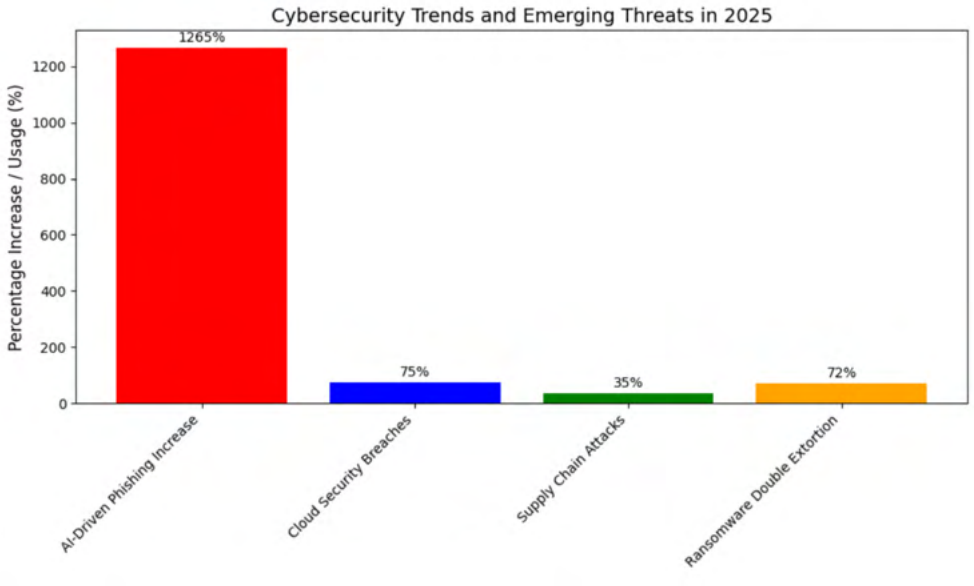
Yet, 32% of nonprofits lack a clear website security plan

35% of nonprofit leaders admit they are unprepared

Where are the web vulnerabilities?

Trends & Emerging Threats

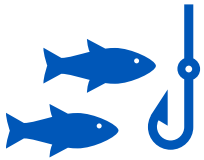
- **AI-Driven Phishing Attacks**: 1,265% increase
- **Cloud Security Breaches**: 75% increase
- **Supply Chain Attacks for Dependencies**: 35% spike
- **Ransomware Double Extortion**: 72% of cases



Sources:
https://sqmagazine.co.uk/cybersecurity-attacks-statistics/
https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

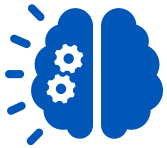
95% of breaches are caused by human error.

Biggest Risks



Phishing &
Credential Theft

Site
Hijacking

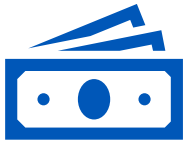


AI-Powered
Attacks

Internet of
Things (IoT)

Mobile
Apps

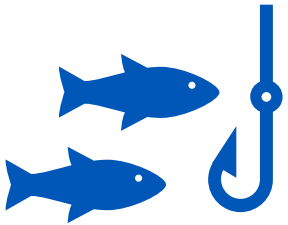
Supply
Chain



Ransomware

Denial of
Service (DDoS)

Biggest Risks



Phishing & Credential Theft

Threat: Phishing emails trick staff into entering login credentials on fake login pages or downloading malware.

- Credential Theft
- Credential Stuffing
- Malware Injection
- Business Email Compromise
- Website Form Exploitation

Impact: Unauthorized changes, data theft, or site defacement.

Biggest Risks

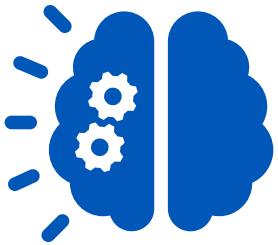
Site Hijacking

Threat: Bad actor obtains admin access to site, host, or domain and steals data, injects site with malware, or redirects domain to nefarious site.

- Session Hijacking from Phishing
- Cross-site Scripting and SQL Injections
- Brute force, weak/exposed passwords, outdated software

Impact: Unauthorized changes, data theft, or site defacement; data manipulation, donor information leaks, or privilege escalation.

Biggest Risks



AI-Powered Attacks

Threat: AI used to identify high-value data and scan websites for vulnerabilities, as well as craft sophisticated campaigns.

- Automated vulnerability scanning
- Deepfake content injection
- AI-driven bot attacks
- Malicious code generation
- AI-Powered Reconnaissance

Impact: Faster, more precise exploitation, data theft, service disruption, silent data exfiltration, increased rate of social engineering and impersonation.

Biggest Risks

Internet of Things (IoT)

Threat: Poorly secured devices become entry points to the network that hosts your website.

- Unsecured devices
- Botnet recruitment
- Cross-device exploits

Impact: Network infiltration, website defacement, data exfiltration, website downtime, ransomware deployment.

Biggest Risks

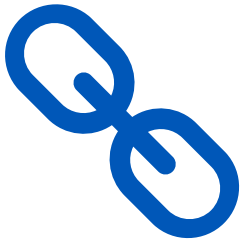
Mobile Apps

Threat: Mobile apps connected to your website via APIs allows bad actors to exploit backend systems.

- Insecure API connections
- Malicious app clones
- AI-driven bot attacks
- Session hijacking
- Data Leakage

Impact: Data breaches / theft, unauthorized content changes, access to website admin, compliance violations.

Biggest Risks



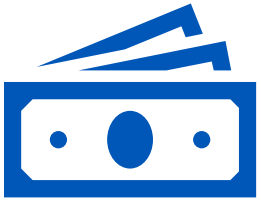
Supply Chain

Threat: Vulnerabilities in integrated third-party web services are exploited and compromise your connected systems.

- Compromised website plugins or CMS tools
- Third-party donation / e-commerce platforms
- File transfer tools
- Malicious code in open-source libraries
- Vendor credential theft

Impact: Data breaches / theft, malware distribution, credential harvesting, PCI compliance violations.

Biggest Risks



Ransomware

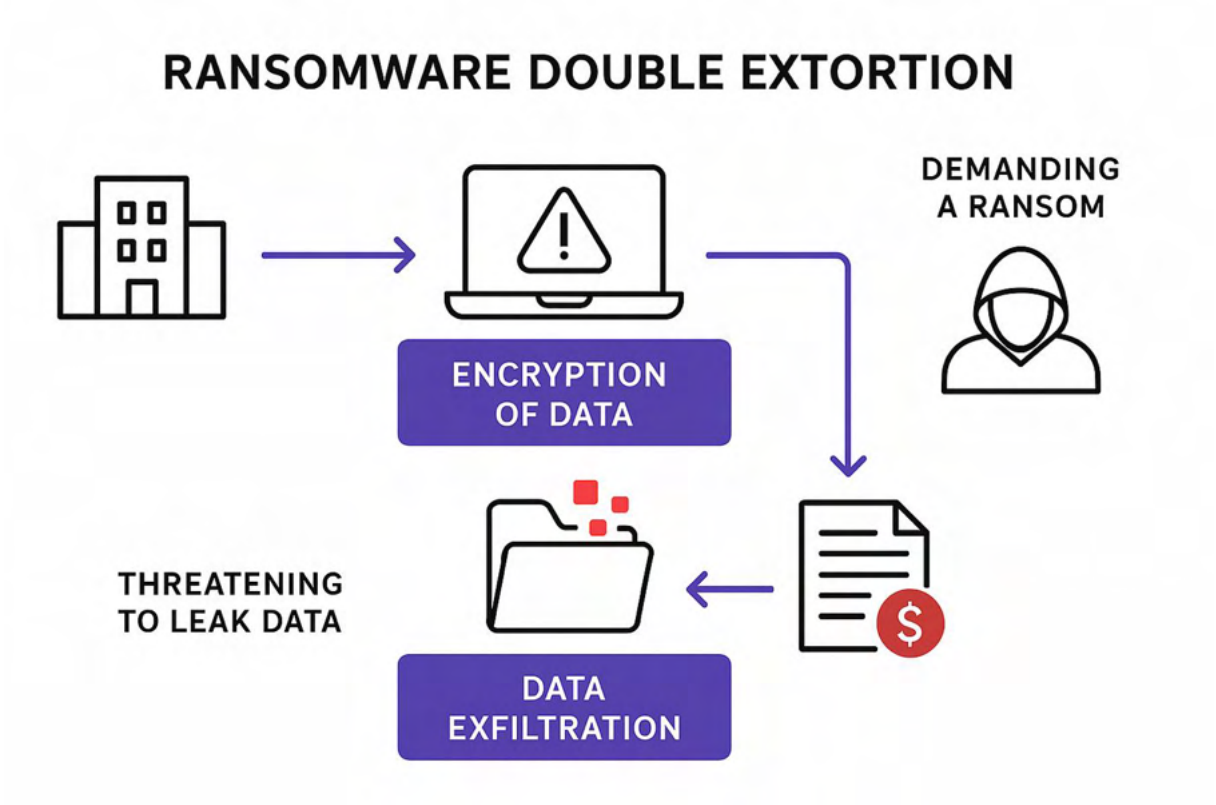
Threat: Attackers exploit outdated CMS platforms or plugins to inject ransomware and lock access to donor databases and operational systems.

- Website server encryption: content, databases
- Admin panel lockout
- Data exfiltration
- Propagation via website plugins
- Disruption of online services

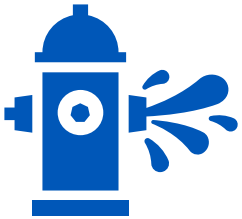
Impact: Financial loss, operational delays, broader compromises, loss of credibility, loss of stakeholder communication.

Biggest Risks

Ransomware



Biggest Risks



Denial of Service (DDoS)

Threat: Attackers flood a website with massive amounts of traffic from multiple sources (often compromised devices or botnets), overwhelming the server and making the site slow or completely inaccessible.

- Website downtime
- Diversion for other attacks
- Resource exhaustion
- Financial costs

Impact: Financial loss, operational delays, increased vulnerability, persistent sluggish performance, reduced engagement.

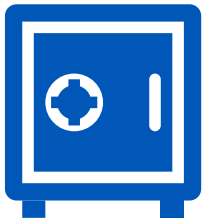
What can you do?

Building a Culture Around Web Security

Policy & Awareness

Human Factors

Web Application



Network & Environment

Building a Culture Around Web Security

Policy & Awareness

- Integrate web and IT oversight
- Engage leadership to fund security measures
- Ensure you own all web-related accounts and assets
- Make web security part of board-level discussions
- Develop clear incident response plans and test
- Develop/update a security policy for digital properties
- Partner with trusted vendors for monitoring & response
- Consider cyber liability insurance to cover breach costs
- Use software bill of materials (SBOM) to track dependencies and updates

Building a Culture Around Web Security

Human Factors

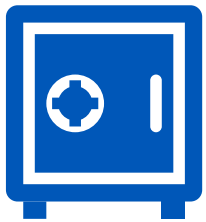
- Raise staff awareness of phishing and best practices
- Provide clear guidelines for staff
- Enforce password hygiene
- Require multi-factor authentication for web admins
- Consider MFA for all authenticating users
- Use least-privilege access controls and role-based permissions

Building a Culture Around Web Security

Web Application

- Audit current website security hygiene: SAST & DAST
- Include security expectations in contracts with vendors
- Configure backup and recovery systems on host
- Ensure regular patching & updates for CMSs
- Limit end user-contributed content
- Employ centralized access controls, if possible
- Enable encrypted connections (SSL/TLS)
- Secure forms with CAPTCHA, input validation

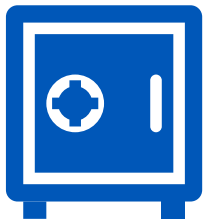
Building a Culture Around Web Security



Network & Environment

- Employ web application firewalls (WAF)
- Employ a Content Delivery Network (CDN)
- Monitor and enable logging in host environment
- Evaluate third-party host security policies
- Monitor third-party integrations
- Perform regular security audits
- Conduct regular penetration testing on web & mobile
- Use AI-based threat detection tools to monitor website traffic and behavior.

Building a Culture Around Web Security



Network & Environment

- Secure all IoT devices with strong credentials and regular firmware updates.
- Use network segmentation to isolate IoT from web servers.
- Implement API security best practices (authentication, rate limiting, encryption) and monitor for threats.
- Monitor mobile app traffic for anomalies and enforce secure coding standards.

Questions?

Thank you!

marcusi@techimpact.org