



Local Business IT Security Audit

Professional Technology Consulting

The Origami Corporation

18.09.2025

Table of Contents

1

Rapid Risk Reduction: Securing a 30-Person Consulting Firm in One Week

1

1.1

Executive Summary

1

1.2

The Challenge

1

1.3

Our Approach

2

1.4

Implementation

3

1.5

Results & Impact

4

1.6

Technologies & Services Used

4

1.7

Conclusion

5

About The Origami Corporation

1 Rapid Risk Reduction: Securing a 30-Person Consulting Firm in One Week

1.1 Executive Summary

After a high-profile breach at a competitor, a 30-employee consulting firm sought to strengthen its security posture and demonstrate resilience to clients. We conducted comprehensive penetration testing across their network and web applications, identified 8 vulnerabilities, and remediated all issues within one week. We then delivered targeted security awareness training and transitioned the firm to our managed services and hardened VPS hosting. Since engagement, the firm has experienced zero security incidents and has passed multiple client security audits with confidence.

Services delivered: penetration-testing, security-hardening, security-awareness-training, vps-hosting, managed-services.

1.2 The Challenge

As the firm grew, so did its exposure. Hybrid work, client data exchange, and a mix of cloud and on-premise systems introduced risk. Following a competitor’s breach, leadership needed assurance of three outcomes: - Validate the resilience of their network and client-facing applications. - Rapidly close any security gaps found—without disrupting business operations. - Establish ongoing controls and evidence to satisfy client security assessments and audits.

Compounding the challenge, the internal IT team was lean and focused on daily operations. The firm required a partner to execute a thorough assessment, imple-

ment fixes quickly, upskill employees on best practices, and provide continuous monitoring and upkeep.

1.3 Our Approach

We applied a pragmatic, standards-aligned program that balanced depth with speed.

- Assessment scope and standards
 - Aligned to NIST CSF and CIS Critical Security Controls for prioritization.
 - Application testing mapped to OWASP Top 10/ASVS.
 - Combined external and internal penetration testing for realistic attack paths.
- Penetration testing methodology
 - Reconnaissance and asset discovery (public footprint, exposed services, cloud endpoints).
 - Vulnerability scanning and manual verification to eliminate false positives.
 - Exploitation attempts with proof-of-concept where safe, followed by risk validation.
 - Secure reporting with clear remediation steps and business impact narratives.
- Security hardening strategy
 - Baseline hardening of servers and network devices against CIS Benchmarks.
 - Identity and access hardening (MFA enforcement, least privilege, credential hygiene).
 - Network filtering, secure remote access, and logging/alerting improvements.
- Security awareness enablement
 - Role-based training emphasizing phishing resistance, data handling, and incident reporting.
 - Practical, scenario-driven exercises relevant to consulting workflows.
- Ongoing protection and assurance
 - Migration of client-facing workloads to a hardened VPS environment.
 - Managed services for patching, monitoring, backup integrity, and periodic security testing.
 - Audit-ready documentation, policies, and evidence collection.

1.4 Implementation

We executed a focused, one-week remediation sprint that integrated findings, fixes, and user enablement with minimal disruption.

Day 1-2: Assessment and validation - Ran external and internal network tests using industry-standard tooling (e.g., Nmap for discovery, OWASP ZAP for web application testing), followed by manual verification. - Uncovered 8 vulnerabilities across infrastructure and application layers. Examples included: - Exposed management service with default or weak controls. - Outdated web application component vulnerable to client-side attacks. - Insecure TLS configuration and missing HTTP security headers on a public endpoint. - VPN configuration allowing legacy protocols and weak cipher suites. - Over-permissive firewall rules and an unpatched server. - Gaps in MFA coverage and stale user accounts. - Prioritized remediation by exploitability and business impact.

Day 3-5: Security hardening and fixes - Patched operating systems and application components; tightened dependency versions. - Implemented MFA across remote access and critical SaaS, and enforced stronger password policies. - Reconfigured firewalls with least-privilege rules; disabled legacy protocols and closed unused ports. - Hardened web servers: enforced TLS 1.2+, HSTS, secure cookies, and appropriate headers; restricted admin interfaces to a VPN/bastion. - Applied CIS-aligned system baselines: service minimization, secure SSH (key-based auth, no root login), log retention, and time sync. - Established centralized log forwarding and alerting thresholds for anomalous authentication and network activity.

Day 5-6: VPS hosting and validation - Migrated the client-facing application to our hardened VPS hosting: - Isolated environment with network segmentation and private services. - Bastion-host access with MFA and IP allowlisting. - Automated backups with encrypted storage and periodic restore tests. - Intrusion prevention (e.g., fail2ban-style controls), file integrity monitoring, and resource telemetry. - Unattended security updates for critical patches and maintenance windows for non-critical updates. - Retested all findings; verified that all 8 vulnerabilities were remediated and that compensating controls were effective.

Day 7: Security awareness and handover to managed services - Delivered a 90-minute, role-based security awareness training session covering phishing indicators, secure data sharing, password/credential hygiene, and incident reporting procedures. - Conducted a baseline phishing simulation to measure readiness and calibrate ongoing training. - Transitioned to managed services: - Monthly vulnerability scans and quarterly light pen tests. - Patch management and configuration drift monitoring. - 24x7 monitoring and alerting, with defined escalation paths. - Backup verification, recovery runbooks, and tabletop exercise scheduling. - Audit support with standardized evidence packs and policy templates.

1.5 Results & Impact

- Rapid remediation: All 8 identified vulnerabilities were fixed within one week, with validation scans confirming no residual exposure.
- Stronger security posture: Hardened configurations, MFA enforcement, and improved network controls reduced the firm's attack surface materially.
- Operational continuity: All work was completed without downtime to client-facing services or internal productivity systems.
- Audit readiness: The firm successfully passed subsequent client security audits, aided by clear documentation, standardized controls, and evidence collected through managed services.
- Cultural shift: Staff demonstrated improved security awareness and responsiveness, with leadership reporting greater confidence in handling vendor due diligence.
- Ongoing assurance: Since the engagement, the firm has reported zero security incidents, supported by continuous monitoring, timely patching, and proactive testing.

Business value realized: - Enhanced client trust and smoother sales cycles due to confident responses to security questionnaires and on-site assessments. - Reduced risk exposure and potential breach costs through layered defenses and continuous oversight. - Predictable operational model for security, turning ad hoc fixes into a managed, measurable program.

1.6 Technologies & Services Used

- Penetration Testing
 - External and internal network testing; web application testing aligned to OWASP Top 10/ASVS.
 - Vulnerability scanning with manual verification; exploit proof-of-concepts where safe.
- Security Hardening
 - CIS-aligned system baselines; secure configuration of VPN, firewalls, and servers.
 - TLS hardening, HTTP security headers, least-privilege access, and service minimization.
 - Centralized logging, alerting thresholds, and secure remote access via bastion.
- Security Awareness Training
 - Role-based training session; baseline phishing simulation; updated incident reporting workflow.

- Reinforcement materials and schedule for ongoing micro-training.
- VPS Hosting
 - Hardened VPS with segmentation, MFA-protected bastion access, and IP allowlisting.
 - Automated, encrypted backups with restore testing; intrusion prevention and integrity monitoring.
 - Controlled patching windows and telemetry for performance and security.
- Managed Services
 - Monthly vulnerability scanning; quarterly light penetration testing.
 - Patch and configuration management; 24x7 monitoring and escalation.
 - Backup verification, recovery runbooks, and audit support with evidence documentation.

1.7 Conclusion

In a single week, the consulting firm moved from concern to confidence. By combining rigorous penetration testing with decisive hardening, practical user education, and a secure VPS hosting foundation, we eliminated immediate risks and established durable, managed defenses. The result is a demonstrably stronger security posture—validated by zero incidents since engagement and successful client audits—delivered through an operating model that scales with the firm’s growth and maintains trust with every engagement.

About The Origami Corporation

The Origami Corporation is a leading technology consulting firm specializing in cloud migration, DevSecOps, cybersecurity, and digital transformation. We help organizations navigate complex technological challenges and achieve their business objectives through innovative, secure, and scalable solutions.

Connect With Us

Follow Us Online

LinkedIn: [The Origami Corporation](#)

Facebook: [@theorigamicorporation](#)

X (Twitter): [@OrigamiGlobal](#)

Telegram: [@theorigamicorporation](#)

Contact Information

Europe & Americas

- **Email:** office@theorigamicorporation.com
- **Phone:** +359 878 686 627

Asia-Pacific, Middle East & Africa (APMEA)

- **Email:** office.apmea@theorigamicorporation.com
- **Phone:** +41 77 924 2245

Ready to Get Started?

SCHEDULE A MEETING

Ready to transform your technology infrastructure? Contact us today to discuss how we can help your organization achieve similar results.