EXPERT WITNESS RESUME

**[Your Full Name]**CEO & Owner, IT Specialists  
Website: itspecialists.net  
Email: [Your Email]  
Phone: [Your Phone Number]

# PROFESSIONAL SUMMARY

Senior IT executive and cybersecurity expert with 14 years of comprehensive IT experience and 10 years specializing in cybersecurity services. CEO and owner of IT Specialists, providing end-to-end managed IT services, cybersecurity solutions, and IT leadership for client organizations. Extensive experience in cyber incident investigation, digital forensics support, and technical consulting alongside cybersecurity insurance firms and legal counsel. Proven expertise in IT governance, infrastructure management, network security, cloud services, and regulatory compliance across multiple industry verticals.

# AREAS OF EXPERTISE

### Cybersecurity & Information Security:

* Cyber Incident Investigation & Digital Forensics Support
* Ransomware Analysis, Containment & Recovery
* Business Email Compromise (BEC) Investigation
* Malware Analysis & Threat Intelligence
* Advanced Persistent Threat (APT) Detection
* Targeted Phishing & Social Engineering Investigation
* Data Breach Response & Notification
* Endpoint Detection & Response (EDR)
* Security Information & Event Management (SIEM)
* Managed Detection & Response (MDR)
* Security Operations Center (SOC) Management
* Zero Trust Network Architecture
* Identity & Access Management (IAM)
* Multi-Factor Authentication (MFA) Implementation
* Privileged Access Management (PAM)
* Vulnerability Assessment & Penetration Testing
* Security Risk Assessment & Management
* Cybersecurity Policy Development & Implementation
* Security Awareness Training & Phishing Simulation
* Incident Response Planning & Tabletop Exercises

### IT Leadership & Operations Management:

* IT Strategy Development & Governance
* Infrastructure Management & Network Administration
* Cloud Services Management
* Virtualization & Containerization Technologies
* Enterprise Architecture & Systems Integration
* IT Service Management (ITSM) & ITIL Processes
* Managed Services Provider (MSP) Operations
* Service Level Agreement (SLA) Management
* IT Budget Planning & Vendor Management
* Help Desk Operations & End-User Support
* Business Continuity & Disaster Recovery Planning
* Backup & Recovery Solutions
* Network Design & Implementation
* Server Administration & Database Management
* Mobile Device Management (MDM) & BYOD Policies
* IT Project Management & Change Management
* Technology Procurement & Lifecycle Management
* Cross-Functional Team Leadership
* Stakeholder Communication & Reporting

### Compliance & Risk Management:

* HIPAA (Health Insurance Portability and Accountability Act)
* PCI-DSS (Payment Card Industry Data Security Standard)
* NIST Cybersecurity Framework Implementation
* GLBA (Gramm-Leach-Bliley Act) Compliance
* CO State Data Breach Notification Laws
* Risk Assessment & Mitigation Strategies
* Audit Preparation & Remediation
* Regulatory Reporting & Documentation

# PROFESSIONAL EXPERIENCE

## CEO & Owner | IT Specialists (itspecialists.net) | 2010 - Present

* Direct comprehensive IT operations and cybersecurity services for client organizations across multiple industry verticals
* Provide end-to-end managed IT services including infrastructure management, network administration, cloud services, and cybersecurity
* Lead cyber incident investigations in collaboration with cybersecurity insurance carriers, legal counsel, and law enforcement
* Specialize in deploying secure access systems for hybrid and remote workforce environments
* Develop and implement IT governance frameworks, policies, and procedures aligned with business objectives
* Manage IT budgets, vendor relationships, and technology procurement for client organizations
* Oversee 24/7 Security Operations Center (SOC) services and managed detection and response capabilities
* Conduct vulnerability assessments, penetration testing, and security risk evaluations
* Design and implement business continuity and disaster recovery solutions
* Provide expert consultation on regulatory compliance requirements and audit preparation
* Lead cross-functional teams and coordinate with stakeholders on complex IT projects
* Deliver technical training and security awareness programs for end-users
* Prepare detailed post-incident reports, technical documentation, and executive briefings

# LEGAL CONSULTING & EXPERT WITNESS EXPERIENCE

Extensive experience providing technical expertise and consultation in legal matters involving cybersecurity incidents, IT operations, and technology disputes. Collaborated with cybersecurity insurance firms, legal counsel, and forensic investigators on:

* Ransomware incident investigation, forensic analysis, and business impact assessment
* Business email compromise (BEC) fraud investigation and financial loss analysis
* Malware infection analysis, containment strategies, and system remediation
* Data breach investigation, scope determination, and regulatory notification requirements
* Targeted phishing and social engineering attack analysis
* Insider threat investigation and privileged access abuse cases
* IT system failure analysis and root cause determination
* Cybersecurity standard of care evaluation and expert opinions
* Technology contract disputes and service level agreement violations
* Intellectual property theft and trade secret misappropriation involving IT systems
* Employment litigation involving computer forensics and electronic evidence
* Insurance claim evaluation for cyber liability and technology errors & omissions
* Regulatory compliance violations and audit findings remediation
* Post-incident technical reporting, damage assessment, and recovery planning

# TECHNICAL PROFICIENCIES

### Cybersecurity Platforms & Tools:

* Todyl SASE (Secure Access Service Edge), SIEM, MXDR, Zero Trust Network Access, EDR
* Huntress platform: endpoint protection, managed detection and response, M365 security, SIEM
* Microsoft 365 Defender, Azure Sentinel, and Microsoft Security Stack
* Tenable, Connect Secure, M365 vulnerability management platforms
* Metasploit, vPenTest, Kali penetration testing tools
* Duo Security, Okta, Azure AD identity and access management
* MailProtector, Proofpoint, Barracuda email security solutions
* Palo Alto Networks, Ubiquiti, Cisco ASA/Meraki firewall management
* Wireshark, tcpdump, and network traffic analysis tools

### IT Infrastructure & Cloud Technologies:

* Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform
* VMware vSphere, Hyper-V, Citrix virtualization platforms
* Microsoft Active Directory, Exchange Server, SharePoint
* Cisco, HP networking equipment and management
* Dell, HP, Lenovo server hardware and management systems
* Veeam, Acronis, Datto backup and recovery solutions
* ConnectWise, Autotask, MSP management tools
* Ninja RMM, Webroot, Kaseya, remote monitoring and management
* Splashtop, Teamviewer, Bomgar remote access
* ActivTrak, Teramind Productivity Monitoring Software

### Industry Experience & Specializations:

* Software Development & Technology Companies
* Healthcare & HIPAA-Regulated Organizations
* Financial Services & Banking
* Legal & Professional Services
* Manufacturing & Industrial
* Education & Research Institutions
* Non-Profit Organizations
* E-commerce & Retail
* Remote & Hybrid Workforce Environments

# PUBLICATIONS & THOUGHT LEADERSHIP

Regular contributor to cybersecurity and IT management blog at itspecialists.net, providing industry insights, threat analysis, best practices, and commentary on emerging cybersecurity trends, regulatory developments, and technology innovations.

# PROFESSIONAL QUALIFICATIONS

* 14 years of comprehensive IT leadership and management experience
* 10 years of specialized cybersecurity and information security focus
* CEO and business owner with profit & loss responsibility
* Extensive hands-on experience with enterprise cybersecurity and IT infrastructure
* Proven track record in cyber incident investigation and digital forensics support
* Experience collaborating with legal counsel, insurance carriers, and law enforcement
* Strong technical writing, documentation, and executive communication skills
* Cross-industry experience with regulatory compliance and audit requirements
* Managed services provider operations and client relationship management
* Team leadership and cross-functional project management expertise

# EXPERT WITNESS CAPABILITIES

* Technical analysis and interpretation of cybersecurity incidents and IT system failures
* Assessment of cybersecurity policies, procedures, and implementation effectiveness
* Evaluation of industry standard practices, regulatory compliance, and duty of care
* Expert opinions on breach causation, attack vectors, and preventive measures
* Analysis of IT infrastructure design, implementation, and operational practices
* Damage assessment and business impact analysis for cyber incidents
* Technology contract review and service level agreement evaluation
* Vendor performance assessment and technology due diligence
* Clear communication of complex technical concepts to legal professionals and juries
* Detailed expert report preparation, affidavit drafting, and deposition testimony
* Case strategy consultation and technical discovery support
* Demonstrative evidence preparation and courtroom presentation

# RELEVANT CASE TYPES

* Data Breach & Privacy Violations
* Ransomware & Cyber Extortion
* Business Email Compromise & Wire Fraud
* Intellectual Property Theft & Trade Secret Misappropriation
* Employment Litigation & Computer Forensics
* Technology Contract Disputes
* Cyber Insurance Claims & Coverage Disputes
* Regulatory Compliance Violations
* Professional Malpractice (Technology)
* Product Liability (Software/Hardware)
* Corporate Espionage & Insider Threats
* Technology Due Diligence & M&A Disputes