Another Great Zero-Trust Resource – NIST Provides Updated Guidance

By Michael C. Maschke, Sharon D. Nelson, Esq., and John W. Simek

The National Institute of Standards and Technology (NIST) is an excellent resource for businesses seeking guidance and instruction to secure their information systems. This month, NIST dropped SP 1800-35, a practical practice guide boasting 19 real-world zero-trust example implementations using off-the-shelf technology from big-name vendors. It is a great starting point for firms of all sizes when developing Zero Trust architecture.

Why This Matters

Traditional cybersecurity followed a set-it-and-forget-it mantra – keep the bad guys out, and we're good. Firewalls were the defender that many firms solely relied upon. That doesn't cut it anymore. As NIST points out, modern networks are hybrid beasts: cloud servers, employee homes, airport Wi-Fi, mobile devices—you name it. Consequently, cybersecurity threats don't just knock at the front door; they're looking for every possible way into your systems and environment.

Zero Trust flips the script. Instead of trusting the perimeter, it uses a "Trust No One " approach to treat every access request with suspicion. This is especially critical in a remote technological environment, where users and information live and are accessed outside the traditional perimeter. Zero Trust evaluates users, devices, and locations based on identity, device posture, behavior, geolocation, and more before granting access. For attorneys handling sensitive data, privileged communications, case materials, and client information, this granular access control is essential to keeping your information safe. Switching from traditional cybersecurity approaches to Zero Trust requires a change to a risk-based approach, planning, and careful implementation.

This latest guide provides plug-and-play architectures you can adapt to your firm. It includes the technology, workflows, and security settings and controls behind each architecture and scenario, plus best practices and lessons learned. You can choose which architecture best fits your firm's environment, whether it's Microsoft 365, Google, or Cisco. The guides also assume your technology environment is hybrid, meaning both cloud and on-prem, demonstrating how zero-trust works for your configuration. It also stresses that adopting Zero Trust is a journey and does not happen overnight. Firms must start somewhere – why not start with your most sensitive data and move on from there? Taking the first step is always the most challenging part.

Key Takeaways

- **Map your assets.** Identify high-value data —client portals, cloud-based file storage, managing partner systems—and define who can access them, and under what conditions.
- **Start small.** You don't need to overhaul everything. Pick somewhere to start—maybe secure your remote document repository using identity governance and micro-segmentation.
- **Run audits and monitoring.** Constant verification means logs, analytics, and alerts, ensuring that you catch suspicious access early and maintain an audit trail for ethical compliance.
- **Rely on best practices.** Instead of reinventing the wheel, you can follow NIST's step-by-step builds. The guide even includes lessons learned from vendors to help avoid common pitfalls.

Law firms should continue to strive to implement the best practices regarding cybersecurity measures to protect their client data. Law firms often rely on what's reasonable when making cybersecurity and technology-related decisions.

Zero Trust architecture is quickly becoming a "reasonable" solution to implement. It may shortly be required by clients, cyberinsurance companies, and government and state regulations to protect the confidentiality of the sensitive information law firms store and maintain. Very soon, Zero Trust won't be just a reasonable solution – it will be mandatory – so get started now.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com*