PROJECT GREEN WALL

by Sarah Anderson

The Story

Most stories do not begin at the sequel, but Green Wall grew from a successful solo law practice. In 2017, Green Wall founder, Sarah Anderson was sitting in a San Francisco ballroom realizing that her former practice area was trending towards a Lehman Brothers-style end. Learning cyber law through Army service, Sarah decided to leave her "big law" partnership and launch a cyber law practice from scratch with SWA Law LLC and LegallyCyber.com.

Despite military deployments and a pandemic, the practice grew and included speaking events, at which someone usually asked: "Where can we send our people to learn more about cyber law?" Realizing the answer was "nowhere," Sarah began developing pragmatic education on technology law issues and incident response. Without delays caused by academic accreditation bodies, Sarah incorporated real-time research and legislative changes into the training materials. Today, Green Wall capitalizes on knowledge from 150+ cyber incidents and legal research to deliver a vibrant and effective professional education.

The Pitch

Most industry professionals lack sufficient cybersecurity consciousness to effectively manage resources and combat modern cyber threats. Blind reliance on a single employee or outside vendor to protect digital assets is an unnecessary vulnerability, as a single cyber-attack can fatally wound any business. Designed for non-technology professionals, the ideal Green Wall student is anyone in an organizational leadership position, who may be impacted by a cyber-attack. If this description seems overly broad, it is because every professional in a leadership position, in every business or government entity, confronts cybersecurity-related issues.

> **Example 1:** Chief Financial Officer of a construction company must advise whether to allocate funds for a remote security operations center versus new heavy construction equipment. An informed decision requires an understanding of current network vulnerabilities and regulated data field requirements. Green Wall teaches minimum network security requirements and risk mitigation from a regulatory and civil liability perspective.
>
> **Example 2:** A Mayor learns that the city's digital infrastructure is under a ransomware attack. Reporters seek comments after news of the incident was leaked by an employee's twitter account. How should the Mayor respond? Should he pay the ransom demand? The Mayor's counsel and public affairs officer never participated in a cyber incident response before. Green Wall courses address public relations issues, offer guidance on law enforcement cooperation, and identify legal restrictions on ransomware payments.

Green Wall's unique pragmatic approach empowers students to make strategic financial and liability mitigation decisions about technology practices.

The Training

Most technology courses are only directed at technology professionals, creating a language barrier between business leaders and their technology support staff. Green Wall Courses conquer the technology language barrier and efficiently enhance an organization's collective power to prevent cyber-attacks and preserve their assets through the following courses taught through relatable and enjoyable presentations:

1. **Cybersecurity Basics – In Lay-Person "English" | 60 Minutes**

   This course addresses three topics, in plain English: 1) The minimum-security requirements for any network; 2) Basic network functionality and cybersecurity tools; and 3) Common cyber threat. In this course, professionals learn to communicate with their technology experts to accurately prioritize resources to enhance cybersecurity for their organization.

2. **Navigating Cyber Insurance | 60 Minutes**

   Cyber insurance is increasingly expensive, but many security experts wonder if policies are worth the money. Cyber insurance policies often contain multiple deductibles, ***strongly*** preferred but expensive vendors, and vary wildly in coverage options. This course outlines minimum coverage items to ensure that any cyber policy is worth the purchase, while providing key guidance for an insured navigating post-event matters with their insurer.

3. **Mitigating Cyber Liability | 90 Minutes**

   With cybersecurity requirements increasingly included in contracts and a cybersecurity due diligence exercise in every merger and acquisition, the absence of appropriate cyber hygiene can not only result in regulatory penalties but also civil litigation. This course provides a realistic perspective on liability, inside and outside of a courtroom, for informed decisions on risk.

4. **Artificial Intelligence Basics and Legal Implications | 60 Minutes**

   This presentation begins by explaining artificial intelligence by breaking it down into two components: data sets and algorithms. The instructor describes general types of artificial intelligence, using pop culture references to help relate the concepts to the audience. Once the audience learns the introductory concepts, the instructor describes the left and right legal limits of use, appealing to attorneys, A.I. consumers, and A.I. developers alike.

5. **The Rise of Social Media Laws | 90 Minutes**

   The dark side of the Social Media is emerging, with lawsuits and data highlighting addictive properties and negative impacts. States are rapidly seeking to limit access to social media by impressionable youth and impose content restrictions for artificial intelligence generated content, while the Federal Government is focusing on threats to National Security. This

presentation impartially identifies the current laws on social media and provides legal predictions for near future.

6. **Third-Party Risk Management | 90 Minutes**

   Apart from employees, vendors represent the biggest security threat to any organization. Vendors are often given too many privileges, both digitally and physically to its hosts network, and lack the contractual restraints to properly apportion liability in the event of a crisis. This course discusses contracts, the zero trust policies, and how to vet vendors before granting them network access.

7. **Building Internal Cyber Assurance Programs | 90 Minutes**

   Whether called a Cyber Assurance Program or Cybersecurity Policy, the desired end-goal is the same: a reliable source of protocols that continually enforce and improve an organization's cybersecurity efforts. This course describes how to create a cohesive cyber ecosystem through internal knowledge and do's and don'ts, and further discusses the introduction of artificial intelligence, employee policies, and information management.

8. **Cyber Incident Response Plans | 180-240 Minutes**

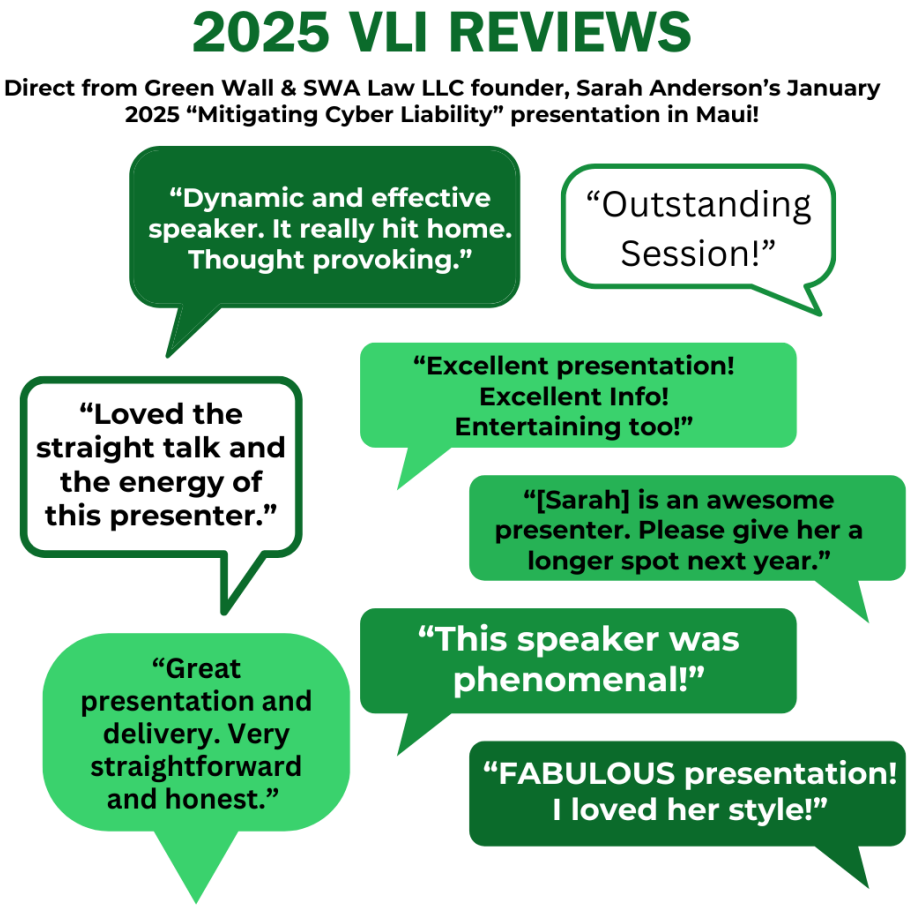
   This course explains the content and purpose behind a cyber incident response plan (CIRP) and helps create a CIRP for each organization that reflects its internal structure, personnel, and existing vendor agreements. The CIRP is intended to be short, effective, and allow any reader to navigate a crisis quickly and get the right information to the right personnel. These plans also include guidance on public relations and internal communications with an eye on mitigating liability.

The Advantages

Green Wall courses are exclusively created and delivered by Sarah Anderson, a nationally recognized subject matter expert, who combines humor, pop culture references, and clarity to a boring and complicated series of topics. Additional advantages include the following:

- Ability to train multiple personnel in an environment curated to the client's specific business and industry.
- Created to pragmatically mitigate cyber liability and increase business recovery.
- Short courses provide an immediate ROI for employers by quickly returning equipped and confident participants to the workplace.
- Green Wall prices courses based on hours of instruction and numbers of participants, allowing organizations to build a training option that fits their needs and budgets. Alternatively, traditional higher education programs offering degrees and certificates in cyber policy require multi-year time commitments and prices between $17,000-$89,000.00 per participant.[1] Higher-Ed programs are also theoretical and risk stagnation given accreditation standards.

Sarah Anderson consistently receives rave reviews from diverse audiences composed of bankers, IT providers, small business owners, and attorneys alike:



For more reviews, please visit: https://www.lawline.com/course/cyber-liability-cybersecurity-for-lawyers-and-law-firms

[1] New York University M.S. in Cyber Risk and Strategy: $89,430.00 (2024); University of Maryland M.S. in Cybersecurity Law: $28,500.00 (2024); Indiana University Cybersecurity Law and Policy Certificate: $17,016.00 (2024).

Sarah Anderson

Sarah@LegallyCyber.com | 225.615.0810

Sarah W. Anderson founded SWA Law LLC. Assisting with over 150 cyber incident responses, Sarah advises leaders and technology professionals on preventing and mitigating liability before, during, and after a cyber incident. Sarah consistently monitors state and federal law on emerging issues such as artificial intelligence and social media. Sarah is licensed to practice in four (4) states: Louisiana, Texas, Pennsylvania, and Illinois.

Prior to SWA Law, Sarah was in-house counsel with a technology non-profit, assisting with intellectual property and federal contracts. During her years as a "big law" partner, Sarah focused on toxic tort and property litigation.

Formerly, Sarah served as the chief legal counsel for the State of Louisiana ESF-17 (Cyber Incidence Response), Cyber Law Judge Advocate for the Louisiana National Guard, and Legal Liaison for the Louisiana Cybersecurity Commission.

Sarah is a veteran, serving as a Lieutenant Colonel in the U.S. Army Reserves. She previously earned her Airborne Wings and a Combat Action Badge during her time in Iraq.

Education:

- 2006: Graduated *magna cum laude* from the University of Georgia Honor's College and a Distinguished Military Graduate.
- 2009: Graduated *cum laude* from Louisiana State University Paul M. Hebert Law Center.
- 2017: Harvard University Program on Negotiations.
- 2018: SANS Institute, Law of Data Security and Investigations.

Certifications & Experience

- United States Secret Service Director Honor's Award for Cybersecurity.
- GIAC Certified – Law of Data Security and Investigations from SANS Institute.
- Supported and/or managed 150+ Cyber Incidents, including MOVEit exploit.
- Author of cyber legislation and reference guide for Louisiana and CISA CR911 program.
- Speaker/Professional cybersecurity legal educator for following entities, including the Louisiana Supreme Court:
  - Justia, Lawline, WestLegalEd, CUNA, MyLawCLE, SproudEd, Louisiana Hospital Association, Louisiana Dental Association, LSU Law, Louisiana Judicial College, National Governors' Association, Louisiana Governors' Office of Homeland Security, Alabama Military Law Symposium, and local ISACA chapters and chambers of commerce.
- Advised Louisiana and Wyoming Governors on the National Governor's Association Cybersecurity Policy Council.