LEG523: **Law of Data Security and Investigations**

GLEG
Law of Data Security & Investigations
giac.org/gleg

5 Day Program	30 CPEs	Laptop Not Needed

You Will Be Able To

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams

Who Should Attend

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology managers
- Vendors
- Compliance officers
- Law enforcement personnel
- Privacy officers
- Penetration testers
- Cyber incident and emergency responders around the world (including private sector, law enforcement, national guard, civil defense and the like)

"I wish I'd taken LEG523 four years ago, so that our policy and governance could have been enhanced sooner."

— Tom Siu, **Case Western Reserve University**

LEG523 is constantly updated to address changing trends and current events. Here's a sampling of what's new:

- Facing a cyber crisis? File a lawsuit in the courts of another country.
- The arrest and criminal indictment of two Coalfire penetration testers in Iowa
- How to balance the right to data privacy versus the right to data security under GDPR and the new California Consumer Privacy Act
- Invoking attorney-client privilege to maintain confidentiality of security assessments such as penetration tests
- Court decision shows how to improve an official investigation using artificial intelligence.
- Unique and indispensable training for General Data Protection Regulation Officers.
- Form contract to invite outside incident responders – including police, contractors, National Guard, or civil defense agencies from anywhere in the world – to help with a cyber crisis.

New law on privacy, e-discovery and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies, and records management procedures.

This course covers the law of fraud, crime, policy, contracts, liability, IT security and active defense—all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues or other investigations.

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Fundamentals of Data Security Law and Policy

The first section is an introduction to law and IT that serves as the foundation for discussions during the rest of the course. We survey the general legal issues that must be addressed in establishing best information security practices, then canvass the many new laws on data security and evaluate information security as a field of growing legal controversy. We will cover computer crime and intellectual property laws when a network is compromised, as well as emerging topics such as honeypots. We will look at the impact of future technologies on law and investigations in order to help students factor in legal concerns when they draft enterprise IT security policies. For example, students will debate what the words of an enterprise policy would mean in a courtroom. The course also dives deep into the legal question of what constitutes a "breach of data security" for purposes of notifying others about it or for other reasons. The course includes a case study on the drafting of policy to comply with the Payment Card Industry Data Security Standard (PCI). Students learn how to choose words more carefully and accurately when responding to cybersecurity questionnaires from regulators, cyber insurers and corporate customers.

SECTION 2: E-Records, E-Discovery and Business Law

IT professionals can advance their careers by upgrading their expertise in the hot fields of e-discovery and cyber investigations. Critical facets of those fields come forward in course section two. We will focus on the use of computer records in disputes and litigation, with a view to teaching students how to manage requests to turn over e-records to adversaries (i.e., e-discovery), manage implementation of a "legal hold" over some records to prevent their destruction, and coordinate with legal counsel to develop workable strategies to legal challenges. Transactions that used to be conducted on paper are now done electronically, so commercial law now applies to computer security. The IT function within an enterprise has become the custodian of an enterprise's business records. You will learn how to craft sound policy for the retention and destruction of electronic records like email, text messages, and social networking interactions. We will provide methods for balancing the competing interests in electronic records management, including costs, risks, security, regulations and user cooperation. Law and technology are changing quickly, and it is impossible for professionals to comprehend all the laws that apply to their work. But they can comprehend overarching trends in law, and they can possess a mindset for finding solutions to legal problems. A key goal of this course day is to equip students with the analytical skills and tools to address technology law issues as they arise, both in the United States and around the world. Special attention is devoted to European data protection laws (see the white paper by Benjamin Wright on the European Union's new General Data Protection Regulation). The course is chock full of actual court case studies dealing with privacy, computer records, digital evidence, electronic contracts, regulatory investigations, and liability for shortfalls in security. The purpose of the case studies is to draw practical lessons that students can take back to their jobs.

SECTION 3: Contracting for Data Security and Other Technology

Section three focuses on the essentials of contract law sensitive to the current legislative requirements for security. Compliance with many of the new data security laws requires contracts. Because IT pulls together the products and services of many vendors, consultants, and outsourcers, enterprises need appropriate contracts to comply with Gramm-Leach-Bliley, HIPAA, GDPR, PCI-DSS, data breach notice laws and other regulations. The section provides practical steps and tools that students can apply to their enterprises and includes a lab on writing contract-related documents relevant to the students' professional responsibilities. (The lab is an optional, informal "office hours" discussion with the instructor at the end of the day when the course is delivered live.) You will learn the language of common technology contract clauses and the issues surrounding those clauses, and become familiar with specific legal cases that show how different disputes have been resolved in litigation. Recognizing that enterprises today operate increasingly on a global basis, the course teaches cases and contract drafting styles applicable to a multinational setting. Contracts covered include agreements for software, consulting, nondisclosure, outsourced services, penetration testing, and private investigation services (such as cyber incident response). Special emphasis is applied to cloud computing issues. Students will also learn how to exploit the surprising power of informal contract records and communications, including cybersecurity questionnaires and requests for InfoSec assurances.

SECTION 4: The Law of Data Compliance: How to Conduct Investigations

Information security professionals and cyber investigators operate in a world of ambiguity, rapid change, and legal uncertainty. To address these challenges, this course section presents methods to analyze a situation and then act in a way that is ethical and defensible and reduces risk. Lessons will be invaluable to the effective and credible execution of any kind of investigation, be it internal, government, consultant, security incident, or any other. The lessons also include methods and justifications for maintaining the confidentiality of an investigation. The course surveys white-collar fraud and other misbehaviors with an emphasis on the role of technology in the commission and prevention of that fraud. It teaches IT managers practical and case-study-driven lessons about the monitoring of employees and employee privacy. IT is often expected to "comply" with many mandates, whether stated in regulations, contracts, internal policies or industry standards (such as PCI-DSS). This course teaches many broadly applicable techniques to help technical professionals establish that they and their organizations are in fact in compliance, or to reduce risk if they are not in perfect compliance. The course draws lessons from models such as the Sarbanes-Oxley Act. As IT security professionals take on more responsibility for controls throughout an enterprise, it is natural that they worry about fraud, which becomes a new part of their domain. This day covers what fraud is, where it occurs, what the law says about it and how it can be avoided and remedied. Indeed, the primary objective of Sarbanes-Oxley is not to keep hackers out; it is to snuff out fraud inside the enterprise. Scattered through the course are numerous descriptions of actual fraud cases involving technology. The purpose is to acquaint the student with the range of modern business crimes, whether committed by executives, employees, suppliers or whole companies. More importantly, the course draws on the law of fraud and corporate misconduct to teach larger and broader lessons about legal compliance, ethical hacking and proper professional conduct in difficult case scenarios. Further, the course teaches how to conduct forensics investigations involving social, mobile and other electronic media. Students learn how to improve the assessment and interpretation of digital evidence, such as evidence of a breach or other cyber event.

SECTION 5: Applying Law to Emerging Dangers: Cyber Defense

Knowing some rules of law is not the same as knowing how to deal strategically with real-world legal problems. This section is organized around extended case studies in security law: break-ins, investigations, piracy, extortion, rootkits, phishing, botnets, espionage and defamation. The studies lay out the chronology of events and critique what the good guys did right and what they did wrong. The goal is to learn to apply principles and skills to address incidents in your day-to-day work. The course includes an in-depth review of legal responses to the major security breaches at TJX, Target, and Home Depot, and looks at how to develop a Bring Your Own Device (BYOD) policy for an enterprise and its employees. The skills learned are a form of crisis management, with a focus on how your enterprise will be judged in a courtroom, by a regulatory agency, or in a contract relationship. Emphasis will be on how to present your side of a story to others, such as law enforcement, Internet gatekeepers, or the public at large, so that a security incident does not turn into a legal fiasco. In addition to case studies, the core material will include tutorials on relevant legislation and judicial decisions in such areas as privacy, negligence, contracts, e-investigations, computer crime and offensive countermeasures. LEG523 is increasingly global in its coverage, so although this course day centers around U.S. law, non-U.S. law and the roles of government authorities outside the United States will be examined, as well. At the end of this course section, the instructor will discuss a few sample questions to help students prepare for the GIAC exam associated with this course (GLEG).

Course Preview available at: **sans.org/demo**