Digital Forensics, Law and Ethics

Ryan Coon

CYB-535

Dr. Edward Marchewka

February 5, 2025

Part 1:

**What is the purpose of digital forensics?**

The primary purpose of digital forensics is to identify, preserve, analyze, and present data in a manner that is legally acceptable in the context of investigations involving computer crimes. Digital forensics helps uncover evidence that can be used in criminal or civil cases, often involving data recovery from digital devices, network logs, and other electronic sources.

**Explain why it is important for any organization to sustain a permanent digital forensics team.**

Having a permanent digital forensics team is crucial for any organization due to several reasons:

Rapid Response - Cyber incidents can happen at any time, and having a dedicated team ensures a swift response to mitigate damage.

Expertise - A permanent team develops specialized skills and knowledge over time, improving the organization's ability to handle sophisticated cyber threats.

Compliance and Risk Management - As regulations around data protection tighten, a dedicated team helps ensure compliance with laws and regulations, reducing legal risks.

Incident Analysis and Prevention - Continuous monitoring and analysis of incidents can lead to improved security measures and protocols, preventing future breaches.

**In digital forensics, must all investigations follow the same basic methodology? Justify your rationale and explain the steps involved in this methodology.**

Not all investigations must follow the same basic methodology due to the unique nature of each case. However, a widely accepted framework includes:

1. Identification - Determine the scope of the investigation and identify the devices and data sources involved.
2. Preservation - Securely collect and preserve the digital evidence to prevent alteration or loss, often creating bit-for-bit images of storage media.
3. Analysis - Examine the preserved data using forensic tools to uncover relevant information, patterns, or anomalies.
4. Documentation - Maintain detailed records of the entire process, including evidence collection, analysis methods, and findings, to ensure transparency and credibility.
5. Presentation - Present the findings in a clear and understandable manner, often in a court of law, to support legal proceedings.

**Concerning digital forensics, list the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data. Note: This information can be presented in a table or chart.**

|  |  |  |
| --- | --- | --- |
| Law/Policy | Description | Major Components |
| Computer Fraud and Abuse Act (CFAA) | Addresses computer fraud and related activity in the U.S. | Prohibits unauthorized access to computers and data. |
| Health Insurance Portability and Accountability Act (HIPAA) | Protects sensitive patient information in the healthcare sector. | Establishes standards for data privacy and security. |
| Gramm-Leach-Bliley Act (GLBA) | Regulates the collection and disclosure of personal financial information. | Requires financial institutions to protect consumer data. |
| General Data Protection Regulation (GDPR) | EU regulation on data protection and privacy. | Mandates data protection measures and consumer rights. |
| Federal Information Security Management Act (FISMA) | Requires federal agencies to secure information systems. | Establishes a framework for ensuring information security. |

**Examine the U.S. federal laws and legal issues associated with cyber threats, especially cyber types such as fraud and financial cybercrimes.**

U.S. federal laws addressing cyber threats include:

Computer Fraud and Abuse Act (CFAA) - Targets unauthorized access to computers and data, punishing various forms of cyber fraud.

Electronic Communications Privacy Act (ECPA) - Protects wire, oral, and electronic communications while in transit and storage.

Identity Theft and Assumption Deterrence Act - Criminalizes identity theft and provides penalties for those who misuse personal identity information.

Cybersecurity Information Sharing Act (CISA) - Encourages sharing of cybersecurity threat information between private and public sectors to enhance defense against cyber threats.

**Using the organization you selected in Topic 1, discuss the legal rights of the organization to perform forensic investigations on personal mobile devices that are part of your BYOD policy.**

In the context of an organization implementing a Bring Your Own Device (BYOD) policy, legal rights to perform forensic investigations on personal mobile devices can be complex. Generally, organizations have the right to conduct forensic investigations on devices that connect to their networks or store corporate data. This is contingent upon the existence of a clear, communicated policy that informs employees about the extent of monitoring and the organization's rights regarding data access. For instance, if an organization clearly states in its BYOD policy that it reserves the right to access and investigate any data on personal devices used for work purposes, it can legally perform forensic examinations when necessary. However, organizations must balance this with privacy concerns and ensure compliance with applicable laws, such as the Electronic Communications Privacy Act (ECPA), which protects personal communications. Additionally, obtaining consent from employees helps mitigate legal issues and reinforces transparency in the organization's practices (Parr & Brown, 2021).

Part 2:

In many situations, multiple levels of government must work in partnership when ensuring security compliance. As a cybersecurity professional, research the following:

**Describe the federal, state, and local cyber defense partners/structures.**

**Federal Level:**

* Cybersecurity and Infrastructure Security Agency (CISA) - CISA is the primary federal agency responsible for coordinating national cybersecurity efforts. It collaborates with various federal agencies, state governments, and private sectors to manage cyber risks and enhance resilience.
* Department of Homeland Security (DHS) - DHS plays a crucial role in overseeing national cybersecurity initiatives and works closely with CISA and other federal entities to strengthen the nation’s cyber defenses.

**State Level:**

* State Cybersecurity Offices - Many states have established dedicated cybersecurity offices that focus on protecting state infrastructure and data. These offices work in partnership with CISA and local governments to implement tailored cybersecurity strategies.
* Statewide Information Security Programs - These programs ensure that state agencies comply with federal standards and best practices, often providing resources and guidance for local entities.

**Local Level:**

* Local Government Cybersecurity Teams - Local governments often have their own cybersecurity teams that protect municipal systems and data. They collaborate with state and federal partners for resources and best practices.
* Community Engagement - Local governments may engage with community organizations and businesses to promote cybersecurity awareness and best practices, fostering a culture of security at the grassroots level.

**Examine the laws, regulations, and standards that organizations use to align with government requirements around cybersecurity best practices within their industry.**

Organizations must adhere to various laws and regulations to align with government requirements.

NIST Cybersecurity Framework - A voluntary framework that provides guidelines for managing cybersecurity risks, helping organizations to improve their security posture.

Federal Information Security Management Act (FISMA) - Requires federal agencies to secure their information systems and report on their security status, ensuring accountability and transparency.

Health Insurance Portability and Accountability Act (HIPAA) - Sets standards for protecting sensitive patient information in the healthcare sector, ensuring confidentiality and security of medical records.

Gramm-Leach-Bliley Act (GLBA) - Requires financial institutions to explain their information-sharing practices to customers and safeguard sensitive data.

**Explain federal laws and authorities, including the Computer Security Act, Sarbanes – Oxley, Gramm – Leach – Bliley, Privacy (COPPA) HIPAA / FERPA, USA Patriot Act, Americans with Disabilities Act, Section 508, and other Federal laws and regulations.**

Computer Security Act of 1987 - This act directs the National Bureau of Standards to establish a computer standards program for federal systems, enhancing the security and privacy of sensitive information.

Sarbanes-Oxley Act (SOX) of 2002 - Aimed at protecting investors from fraudulent financial reporting, SOX mandates strict reforms to enhance corporate governance and financial disclosures.

Gramm-Leach-Bliley Act (GLBA) - Enacted to protect consumers' personal financial information held by financial institutions, requiring them to implement privacy policies.

Children’s Online Privacy Protection Act (COPPA) - This law imposes requirements on websites and online services directed at children under 13, ensuring parental consent for data collection.

Health Insurance Portability and Accountability Act (HIPAA) - Establishes national standards for the protection of health information, ensuring confidentiality and security of medical records.

Family Educational Rights and Privacy Act (FERPA) - Protects the privacy of student education records and gives parents certain rights regarding their children’s records.

USA PATRIOT Act - Enacted to deter and punish terrorist acts, this act enhances law enforcement investigatory tools and information sharing.

Americans with Disabilities Act (ADA) - While primarily focused on preventing discrimination against individuals with disabilities, it also has implications for digital accessibility in cybersecurity practices.

Section 508: Requires federal agencies to make their electronic and information technology accessible to people with disabilities, impacting how cybersecurity measures are implemented.

Part 3:

For each scenario, identify the applicable law(s) it would fall under and describe how the type of legal dispute (civil, criminal, or private) affects the evidence used to resolve it. **Note:** This information can be presented in a table.

* Transmission of underage photographs to various email addresses in California, Arizona, and Colorado
* Colonial Pipeline Hack
* Victim's identity used to open a new account
* Bank fraud/scam
* A firm's credit card records are stolen

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Applicable Law(s) | Type of Legal Dispute | Effect on Evidence |
| Transmission of Underage Photographs | California Penal Code § 311.2 (Child Pornography) | Criminal | Evidence must meet the standard of "beyond a reasonable doubt." Police may rely on digital forensics, email logs, and witness statements to establish intent and actions. |
|  | Arizona Revised Statutes § 13-3506 (Sexual Exploitation of a Minor) |  |  |
|  | Colorado Revised Statutes § 18-6-403 (Sexual Exploitation of Children) |  |  |
| Colonial Pipeline Hack | Computer Fraud and Abuse Act (CFAA) | Criminal | Evidence includes digital footprints, IP addresses, and logs. It must show malicious intent. Requires expert testimony to interpret technical data and prove unauthorized access. |
|  | Federal Information Security Management Act (FISMA) |  |  |
| Victim's Identity Used to Open a New Account | Identity Theft and Assumption Deterrence Act (ITADA) | Criminal | Evidence may include financial records, communications, and forensic analysis of account creation. Must establish fraudulent intent beyond a reasonable doubt. |
|  | Fair Credit Reporting Act (FCRA) | Civil | In civil cases, evidence might include credit reports, consumer statements, and documentation of damages, which must meet a preponderance of the evidence standard. |
| Bank Fraud/Scam | Bank Fraud Statute (18 U.S.C. § 1344) | Criminal | Evidence must prove intent to defraud. May include transaction records, communications, and witness testimonies. Must meet the criminal standard of proof. |
|  | Federal Trade Commission Act | Civil | In civil cases, evidence can involve patterns of deceit and can be based on consumer complaints and transaction records, requiring a lower standard of proof. |
| A Firm's Credit Card Records are Stolen | Gramm-Leach-Bliley Act (GLBA) | Civil | Evidence includes internal security audits, logs of unauthorized access, and records of the breach. Must demonstrate negligence or failure to comply with regulations. |
|  | Computer Fraud and Abuse Act (CFAA) | Criminal | In criminal cases, it must be shown that the theft was intentional and malicious, using the same types of evidence as other hacking cases. |

Part 4:

When providing information assurance, a sound defense strategy does not only look at the legal aspects but also the ethical abuses of abilities on the job.

**There are three main categories of unethical behavior that organizations must seek to minimize: ignorance, accident, and intent. From your research and your professional/personal experience, provide examples of each category and best practices for how to prevent such activities from happening.**

Ignorance - This category encompasses actions taken without full awareness of their ethical implications(Criterion, 2019). For example, a marketing team might unknowingly use an image without proper licensing, violating copyright laws. To combat ignorance, organizations should invest in comprehensive training on ethical conduct, covering topics like intellectual property, data privacy, and conflict of interest. Clear and accessible codes of conduct should be readily available, outlining expected behaviors and consequences for violations. Open communication channels for employees to raise concerns or seek guidance on ethical dilemmas are also crucial.

Accident - This category involves unintentional mistakes that have ethical consequences(Indeed Editorial Team, 2024). For example, a data analyst might accidentally leak sensitive customer information due to a misconfigured spreadsheet. To prevent accidental breaches, organizations should implement strong data security measures, including encryption, access controls, and regular security audits. Regular training on data handling procedures and best practices can also minimize the risk of accidental errors. Encouraging a culture of accountability and open communication about mistakes helps to identify and address issues quickly.

Intent - This category involves deliberate actions taken with the knowledge that they are unethical(Kaptein, 2011). For example, a manager might knowingly falsify performance data to secure a bonus. Preventing intentional unethical behavior requires a strong ethical foundation within the organization. This includes fostering a culture of integrity where ethical conduct is valued and rewarded. Clear and consistent enforcement of ethical policies is essential, with consequences for violations that are fair and transparent. Whistleblower protection programs allow employees to report unethical behavior without fear of retaliation, encouraging a culture of accountability and ethical decision-making.

**What happens when a job task borders on unethical from your personal viewpoint? Is your response to the issue any different than what you discussed above? What behaviors/tasks would an organization find acceptable where your personal viewpoint may not? Select 2–3 scenarios and discuss how you would address them from a Christian worldview. Consider Matthew 18:15–18. How could you apply this to a workplace scenario?**

Scenario 1 - The "Acceptable" Lie: Imagine you're working on a project for a client who's very demanding. Your manager asks you to tell the client that a certain feature will be ready by a specific date, even though you know it's unlikely. While your manager might view this as a necessary "white lie" to keep the client happy, it goes against your personal integrity.

Scenario 2 - The "Necessary" Discrimination: Let's say you're involved in the hiring process for a new position. You're asked to screen candidates based on their religious affiliation, even though this practice is discriminatory. The company might argue it's essential for cultural fit, but you believe in treating everyone with respect and fairness.

Scenario 3 - The "Profit-Driven" Decision: You work for a company that's considering outsourcing a significant portion of its workforce to a country with lower labor costs. While this might benefit the company's bottom line, you believe in ethical treatment of workers and are concerned about the potential impact on employees.

Applying Matthew 18:15-18: This passage from Matthew instructs us to address conflicts directly and privately, seeking reconciliation. In a workplace scenario, this could mean:

Open Communication - If a task feels unethical, it's crucial to have an open conversation with your manager or supervisor. Explain your concerns clearly and respectfully, emphasizing your commitment to the company's success while upholding your personal values(Bluefield University, 2021).

Seek Resolution - Try to understand the manager's perspective and find a solution that aligns with both your values and the company's needs. Perhaps there's a compromise or alternative approach that can be implemented.

Escalate if Necessary - If the issue can't be resolved through direct communication, consider escalating the matter to HR or a higher-level manager(Work, n.d.). Document your concerns and interactions to ensure transparency.

Christian Worldview - A Christian worldview emphasizes honesty, integrity, and compassion. In these scenarios, a Christian might:

Prioritize Truth: Seek to be truthful and transparent in all interactions, even if it means challenging the status quo.

Respect All People: Treat everyone with dignity and respect, regardless of their background or beliefs.

Advocate for Justice: Speak up against practices that are unfair or harmful, even if it's uncomfortable.

**Refer to the ISACA code of conduct. Describe the responsibilities related to the handling of data as it pertains to legal, ethical codes of conduct, and/or agency auditing issues, frameworks, and best practices.**

The ISACA Code of Professional Ethics outlines essential responsibilities for professionals in the fields of information systems and auditing, particularly concerning the handling of data(Pa, 2024). This code emphasizes the importance of integrity, confidentiality, and professional competence, which are crucial for maintaining trust and compliance with legal and ethical standards.

Responsibilities Related to Data Handling

Integrity and Honesty - Professionals must act with integrity and honesty in all data-related activities. This includes ensuring that data is collected, processed, and reported accurately, without misrepresentation or omission.

Confidentiality - The code mandates that professionals protect the confidentiality of information obtained during their work(Iscac, n.d.). This involves implementing appropriate measures to safeguard sensitive data from unauthorized access or disclosure, in compliance with legal requirements such as GDPR or HIPAA.

Compliance with Laws and Regulations - ISACA members are required to adhere to all applicable laws and regulations governing data handling(Lee Et al, 2016). This includes understanding and implementing frameworks that guide ethical data practices, such as the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the U.S.

Professional Competence - Professionals must maintain their knowledge and skills to ensure they can effectively manage data in accordance with current laws and ethical standards. This includes staying updated on best practices and emerging trends in data privacy and security.

Accountability - The code emphasizes the importance of accountability in data handling. Professionals should be prepared to justify their decisions and actions regarding data management, ensuring transparency and ethical conduct.

Frameworks and Best Practices

Data Governance Frameworks - Establishing a robust data governance framework helps ensure that data is managed responsibly and ethically throughout its lifecycle.

Regular Audits - Conducting regular audits can help organizations assess compliance with ethical standards and legal requirements, identifying areas for improvement.

Training and Awareness Programs: Implementing training programs for employees on data handling practices and ethical standards fosters a culture of compliance and integrity.

**InfoSec professionals are under increasing pressure to provide access to information/data without sacrificing security or usability. Explore the challenges of balancing security and usability and what results if there is a lack of balance between the two.**

The challenge is that the internet is designed in a way that makes it almost impossible to browse without leaving traces. Think of it like walking through a forest - you're bound to leave footprints. Those traces are what make the web work, but they can also be used to track our online activity. The goal is to minimize those traces while still making sure we can use the internet effectively. If we go too far in one direction, we risk either sacrificing security or usability. For example, if we make everything super secure, it might be difficult to use. On the other hand, if we make everything super easy to use, we might be sacrificing security. It's a delicate dance, and it's something that InfoSec professionals are constantly working on.

**Describe how you would integrate information assurance and security requirements into an organization's processes and practices.**

Integrating information assurance and security requirements into an organization's processes and practices is essential for safeguarding sensitive data and ensuring compliance with legal and regulatory standards(Sosin, n.d.). A comprehensive approach involves several key steps:

Risk Assessment - Begin by conducting a thorough risk assessment to identify potential vulnerabilities and threats to the organization's information assets. This helps prioritize security measures based on the level of risk associated with different data types.

Policy Development - Establish clear information security policies that outline the organization's commitment to data protection. These policies should cover areas such as data classification, access control, incident response, and acceptable use(BARR, 2024).

Training and Awareness - Implement regular training programs for employees to raise awareness about information security best practices and the importance of data protection. This fosters a culture of security within the organization.

Integration into Business Processes - Ensure that security requirements are integrated into all business processes, from project planning to daily operations. This can be achieved by incorporating security checkpoints in workflows and decision-making processes.

Continuous Monitoring and Improvement - Establish mechanisms for continuous monitoring of security controls and practices. Regular audits and assessments can help identify areas for improvement and ensure compliance with established policies(Sykes, 2024).

Incident Response Planning: Develop and maintain an incident response plan that outlines procedures for addressing security breaches or data loss. This plan should be regularly tested and updated to reflect changes in the threat landscape(SentinelOne, 2024).

**Examine the ethical considerations of ethics and cyberspace, ethical issues, property, availability, rights of others, respect and principles of community, resource use, allocation, and abuse, censorship, ethics-based decision tools, and cybersecurity and social responsibility.**

Ethical Issues - The digital realm raises significant ethical dilemmas, such as the harm to privacy through surveillance and data breaches, and the harm to property through intellectual property theft. Cybersecurity professionals must navigate these challenges while ensuring that their actions do not infringe on the rights of others(Gunarto, n.d.).

Rights of Others - Respecting the rights of others in cyberspace is paramount. This includes acknowledging individuals' rights to privacy, freedom of expression, and access to information. Ethical frameworks must guide professionals in balancing these rights against the need for security and compliance.

Resource Use and Allocation - The allocation of resources in cybersecurity is critical. Organizations must prioritize their resources effectively to protect sensitive data while ensuring that all stakeholders have equitable access to necessary information. Misallocation can lead to vulnerabilities and ethical breaches(Rathnayake, 2024).

Censorship - Censorship in cyberspace poses ethical questions about the limits of free speech and the role of governments and corporations in controlling information(Chin, 2023). Ethical considerations must guide decisions about what content is permissible, balancing the need for security with the right to free expression.

Ethics-Based Decision Tools - Utilizing ethics-based decision tools can help cybersecurity professionals navigate complex scenarios. These tools provide frameworks for evaluating the ethical implications of actions and decisions, ensuring that they align with both legal standards and moral principles.

Cybersecurity and Social Responsibility - Finally, the concept of social responsibility in cybersecurity emphasizes the duty of professionals to protect not only their organizations but also the broader community. This includes advocating for ethical practices, promoting digital literacy, and ensuring that technology serves the public good(Augusta University, n.d.).

References:

*2023 Colorado Revised Statutes :: Title 18 - CRIMINAL CODE (§§ 18-1-101 — 18-26-102) :: Article 6 - OFFENSES INVOLVING THE FAMILY RELATIONS (§§ 18-6-101 — 18-6-805) :: Part 4 - WRONGS TO CHILDREN (§§ 18-6-401 — 18-6-405) :: Section 18-6-403 - Sexual exploitation of a child - legislative declaration - definitions*. (2023). Justia Law. https://law.justia.com/codes/colorado/title-18/article-6/part-4/section-18-6-403/

*Arizona Revised Statutes*. (2019). Azleg.gov. https://www.azleg.gov/arsDetail/?title=13

Artur, S. (n.d.). *HOW TO INCREASE THE INFORMATION ASSURANCE IN THE INFORMATION AGE*. http://www.jodrm.eu/issues/volume9\_issue1/05\_Sosin.pdf

Augusta University. (n.d.). *Cybersecurity Ethics: What Cyber Professionals Need to Know*. Cybersecurity Ethics: What Cyber Professionals Need to Know. https://www.augusta.edu/online/blog/cybersecurity-ethics/

BARR. (2024, January 8). *How to Implement an Information Security Program in 9 Steps - BARR Advisory*. Https://Www.barradvisory.com/. https://www.barradvisory.com/resource/how-to-implement-an-information-security-program-in-9-steps-2/

BlueField University. (2021). *How to Apply Christian Ethics to Business Practices*. Bluefield University. https://www.bluefield.edu/blog/importance-christian-ethics-business/

*California Code, Penal Code - PEN § 311.2 | FindLaw*. (2023). Findlaw. https://codes.findlaw.com/ca/penal-code/pen-sect-311-2/

Chin, K. (2023, August 21). *Cybersecurity and Social Responsibility: Ethical Considerations | UpGuard*. Www.upguard.com; UpGuard. https://www.upguard.com/blog/cybersecurity-ethics

CISA. (2014). *Federal Information Security Modernization Act | CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

*Code of Professional Ethics - New England Chapter*. (2023). Isaca.org. https://engage.isaca.org/newenglandchapter/aboutchapter/new-page

Computer Security Division, I. T. L. (2016, June 10). *CSRC Topic: Federal Information Security Modernization Act | CSRC*. CSRC | NIST. https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma

Criterion. (2019). *Unethical Behavior in the Workplace: 10 Examples and How To*. Criterionhcm.com. https://www.criterionhcm.com/blog/unethical-workplace-behavior

Federal Trade Commission. (n.d.). *Gramm-Leach-Bliley Act*. Federal Trade Commission. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

*Gramm-Leach-Bliley Act (GLBA) Compliance at ECU | University Data Governance | ECU*. (n.d.). Datagovernance.ecu.edu. https://datagovernance.ecu.edu/gramm-leach-bliley-act-glba-compliance-at-ecu/

*Guide to data security standards*. (n.d.). Www.ironmountain.com. https://www.ironmountain.com/resources/blogs-and-articles/g/guide-to-data-security-standards

Gunarto, H. (n.d.). *Ethical Issues in Cyberspace and IT Society*. https://www.apu.ac.jp/~gunarto/it1.pdf

Indeed Editorial Team. (2024). *6 Examples of Ethical and Unethical Behavior (With Tips)*. Indeed Career Guide. https://www.indeed.com/career-advice/career-development/ethical-behavior

Kaptein, M. (2011, May 1). *(PDF) Understanding Unethical Behavior by Unraveling Ethical Culture*. ResearchGate. https://www.researchgate.net/publication/254097714\_Understanding\_Unethical\_Behavior\_by\_Unraveling\_Ethical\_Culture

Lee, W., Zankl, W., & Chang, H. (2016, December 24). *An Ethical Approach to Data Privacy Protection*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection

Pa, S. (2024, January 18). *Code of Conduct: An Effective Tool for GDPR Compliance*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/code-of-conduct-an-effective-tool-for-gdpr-compliance

Parr&Brown. (2013, February 27). *The Legal Side of Bring Your Own Device (BYOD)*. Parr Brown Gee & Loveless. https://parrbrown.com/the-legal-side-of-bring-your-own-device-byod/

Poli, S. (2024). *The Electronic Communications Privacy Act: Law Explained — Vintti*. Vintti.com. https://www.vintti.com/blog/the-electronic-communications-privacy-act-law-explained

Rathnayake, D. (2024). *The Importance of Ethics in Cybersecurity*. Tripwire.com. https://www.tripwire.com/state-of-security/importance-ethics-cybersecurity

SentinelOne. (2024, September 6). *What is Information Assurance? Benefits & Challenges*. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-information-assurance/

Sykes, N. (2024). *Understanding and Implementing Information Assurance in Facilities Portfolio Management and Enterprise Asset Management | R&K Solutions*. Rksolutions.com. https://www.rksolutions.com/resources/understanding-and-implementing-information-assurance-in-facilities-portfolio-management-and-enterprise-asset-management

Team, S. R. (2024, February 14). *Understanding the GLBA Safeguards Rule, 2024 Complete Guide - Isora GRC*. Isora GRC. https://www.saltycloud.com/blog/what-is-glba/

U.S. Department of Health and Human Services. (2022, October 19). *Summary of the HIPAA privacy rule*. HHS.gov; U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

U.S. Department of Justice. (2015, February 19). *Computer Fraud and Abuse Act*. Www.justice.gov. https://www.justice.gov/jm/jm-9-48000-computer-fraud

Wolford, B. (2018). *What is GDPR, the EU’s new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

Work, T. of. (n.d.). *Ethics at Work (Overview)*. Theology of Work. https://www.theologyofwork.org/key-topics/ethics/