

TOPIC	DESCRIPTION
<u>Recap</u>	Second Class

Does a data act or omission cause an impact to a material life interest? Is it net positive or negative?

Key Points

- ❑ Data Ethics
 - ❑ Security & Privacy
 - ❑ Fairness and Justice
 - ❑ Transparency and Autonomy
 - ❑ Deceptive or unfair

Look for

- An act or omission
- Not reasonable
- Significant or material harm

Examine lifecycle

- Collection
- Use*
- Processing
- Protection
- Storage
- Disclosure
- Destruction

* Including downstream use

MSBA 5507.1 Ethics, Risk Management and Data Security

Cyber Security

July 10, 2023



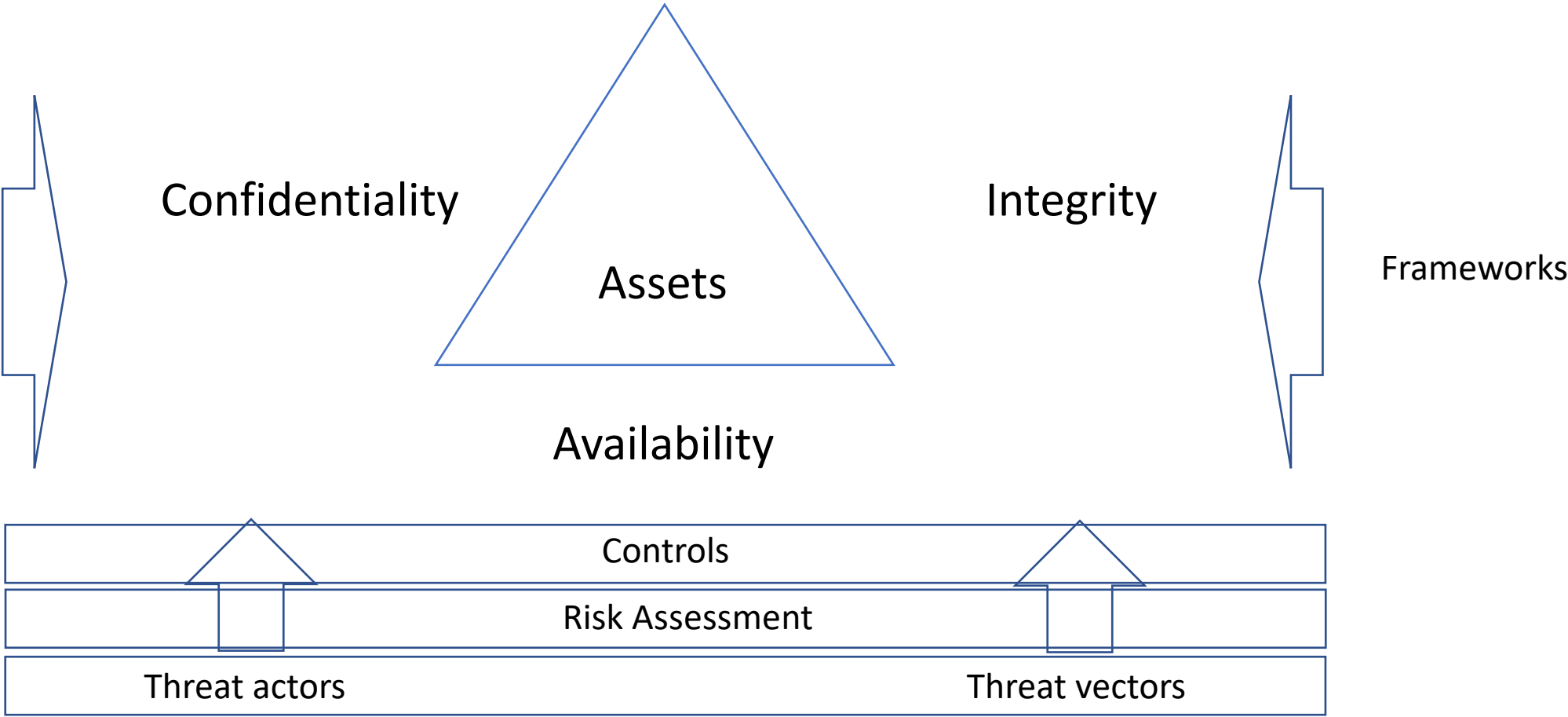
Ken DeJarnette

ken@kdejarnette.com

ken.dejarnette@dominican.edu

213-399-8706

Office hours: Wed 1-3 pm

TOPIC	DESCRIPTION/SOURCES
<p><u>Security</u></p>	<p>Cybersecurity Fundamentals, Study Guide, 3rd Edition, ISACA, ISBN: 978-1-60420-751-4, § 1.13 – 1.15 (Security Overview)</p>
<p><u>Discussion</u></p>	 <p>The diagram illustrates the relationship between security concepts. At the center is a triangle with 'Confidentiality' at the top, 'Integrity' at the bottom right, and 'Availability' at the bottom left. Inside the triangle is the word 'Assets'. To the left of the triangle is a double-headed arrow labeled 'Standards'. To the right is a double-headed arrow labeled 'Frameworks'. Below the triangle is a horizontal bar divided into three sections: 'Controls' (top), 'Risk Assessment' (middle), and a bottom section containing 'Threat actors' on the left and 'Threat vectors' on the right. Small triangles point from the 'Controls' and 'Risk Assessment' sections up towards the central triangle.</p>

TOPIC**DESCRIPTION/SOURCES****Security**

**Cybersecurity Fundamentals, Study Guide, 3rd Edition, ISACA, ISBN: 978-1-60420-751-4,
§ 3.4 (Controls)**

Discussion

Control Type	Control Function			
		Preventative	Detective	Corrective
	Physical			
	Technical/Logical			
	Administrative			

TOPIC**DESCRIPTION/SOURCES****Security**

- **Cybersecurity Fundamentals, Study Guide, 3rd Edition**, ISACA, ISBN: 978-1-60420-751-4, § 3.4.11 – 3.4.13 (Applications, Data & Cloud)
- Travis D. Breaux, **An Introduction to Privacy For Technology Professionals**, (2020), chapter 9 (Cybersecurity and Privacy)

Discussion

	What are key risks?	What are examples of key controls?	What role does/might data science play?
Application			
Data			
Cloud			

TOPIC

DESCRIPTION/SOURCES

Security

Cybersecurity Fundamentals, Study Guide, 3rd Edition, ISACA, ISBN: 978-1-60420-751-4,
§ 3.2 (Standards, Frameworks, Best Practices and Compliance Sources)

- ☐ Standards
- ☐ Frameworks
- ☐ Best practices
- ☐ Compliance/assurance

- ☐ What are they?
- ☐ Why use them?
- ☐ How do you use them?
- ☐ What are examples?

Discussion

NIST Cybersecurity
Framework



TOPIC	DESCRIPTION/SOURCES
<u>Security</u>	<p>Interagency Guidelines Establishing Information Security Standards, FRB FFIEC Information Technology Examination Handbook, Information Security (2016)</p>
<u>Discussion</u>	<ul style="list-style-type: none"> <input type="checkbox"/> What are key attributes of a reasonable financial institution security program? <ul style="list-style-type: none"> <input type="checkbox"/> Comprehensive and written <input type="checkbox"/> Approved and overseen by the BOD (or committee of the BOD) <input type="checkbox"/> Tailored to the complexity of the institution and includes administrative, technical and physical safeguards to: <ul style="list-style-type: none"> <input type="checkbox"/> Ensure the security and confidentiality of customer data <input type="checkbox"/> Protect against anticipated threats and hazards <input type="checkbox"/> Protect against unauthorized access <input type="checkbox"/> Ensure proper disposal of customer information <input type="checkbox"/> Based on an assessment of reasonably foreseeable risks that is ongoing <input type="checkbox"/> Implement controls commensurate with the sensitivity of the information (must consider access, encryption, monitoring, response et al.) <input type="checkbox"/> Includes response, training, testing of key controls programs, along with oversight of third-parties <input type="checkbox"/> Is periodically adjusted

TOPIC	DESCRIPTION/SOURCES
<u>Security</u>	<i>In the Matter of Zoom Communications, Inc.</i> , File No. 192 3167 (F.T.C. Nov 2020)
<u>Discussion</u>	<ul style="list-style-type: none"><input type="checkbox"/> Room One: What security controls were missing?<input type="checkbox"/> Room Two: What is meant by (1) “commonly known or reasonably foreseeable attacks,” (2) “readily available measures to safeguard,” and (3) “systematic process[es]?”<input type="checkbox"/> Room Three: Was Zoom deceptive, and if yes, how (use the specific facts)?<input type="checkbox"/> Room Four: Was Zoom’s security program reasonable?

TOPIC	DESCRIPTION/SOURCES
<u>Security</u>	State Breach Notification Laws, Foley & Lardner LLP (2021)
<u>Discussion</u>	<ul style="list-style-type: none"><input type="checkbox"/> Key Elements<ul style="list-style-type: none"><input type="checkbox"/> Definitions<ul style="list-style-type: none"><input type="checkbox"/> Personal Information<input type="checkbox"/> Breach/Unauthorized Access<input type="checkbox"/> Risk of harm analysis<input type="checkbox"/> Safe harbors<input type="checkbox"/> Notification timing<ul style="list-style-type: none"><input type="checkbox"/> Individuals<input type="checkbox"/> Regulators<input type="checkbox"/> Enforcement<ul style="list-style-type: none"><input type="checkbox"/> Regulators<input type="checkbox"/> Private right of action

TOPIC

DESCRIPTION/SOURCES

Security

California Breach Notification

State of Residence	California
Statute	Cal. Civ. Code § 1798.80 <i>et seq.</i> ; Cal. Health & Safety Code § 1280.15
Definition of “Personal Information”	<p>(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number; (2) driver's license number or California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) medical information; (5) health insurance information; (6) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes; (7) information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.</p> <p>(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.</p>
Definition of “Breach”	<p>Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.</p> <p>Medical Information-Specific Statute Unlawful or unauthorized access to or use or disclosure of a patient's medical information, whether in paper or electronic form, triggers the notification requirement.</p>
Safe Harbor for Data that is Encrypted,	<p>Yes – in certain situations depending on the factual circumstances.</p> <p>Medical Information-Specific Statute</p>
Timing of Notification to Individuals	<p>The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.</p>

TOPIC	DESCRIPTION/SOURCES
<u>Security</u>	Perfect Grocery Case Study
<u>Discussion</u>	<ul style="list-style-type: none"><input type="checkbox"/> Room One: Do you see any confidentiality, integrity or availability issues?<input type="checkbox"/> Room Two: What security controls do you think are missing?<input type="checkbox"/> Room Three: Was there an unauthorized access/breach and why?

TOPIC	DESCRIPTION/SOURCES
<u>Security</u>	Travis D. Breaux, An Introduction to Privacy For Technology Professionals , (2020), chapter 9 (Cybersecurity and Privacy)
<u>Discussion</u>	<p data-bbox="417 344 700 386">Final thoughts</p> <div data-bbox="417 422 1217 1222"> <ul style="list-style-type: none"> <input type="checkbox"/> Be straightforward and train everyone <input type="checkbox"/> Know environment <input type="checkbox"/> Focus on completeness <input type="checkbox"/> Follow least privilege concept <input type="checkbox"/> Layer defenses <input type="checkbox"/> Practice zero trust <input type="checkbox"/> Monitor constantly <input type="checkbox"/> Gather intelligence actively <input type="checkbox"/> Practice preparedness <input type="checkbox"/> Redundancy </div> <div data-bbox="1429 422 2140 1222"> <ul style="list-style-type: none"> ➤ Complexity leads to mistakes, or acceptability/usability issues ➤ Where is sensitive data/critical IP ➤ Lock all the doors ➤ No more than necessary ➤ Access, encryption, segmentation ➤ Multifactor authentication ➤ Egress and Ingress, be vigilant ➤ Patch or fix, design a new control ➤ Fast reaction requires planning ➤ Keep backups/replications safe </div>