Assignment 1 – First Draft Notes

According to NIST xxxx-xxxx

Preparation

- ID purpose of assessment
  - To assess the risk profile of
    - Paws as it currently is
    - Paws if it digitalized its business model
- ID scope
  - Tier 2 and 3?
- ID assumptions/constraints
  - Assumptions:
    - Employees are not trained in cyber defense tactics
      - passwords
      - malicious websites
      - network traffic
    - The network does not have a firewall, VPN, or proxy
    - Devices are not regularly updated
      - the logistics computer
      - the front desk computer
      - employees' personal devices
- ID sources of info used as input
  - Qualitative sources:
    - CAPEC ATT&CK list
    - Secondary sources
  - Quantitative sources:
    - None
- ID risk model, assessment approaches, analytic approaches
  - Risk Model: Octave
  - Profit POV
    - If customer/supplier privacy is at risk, would tank profits, digitization or not
  - Qualitative assessment:
    - STRIDE – Threat taxonomy
    - LIDDUN? – Privacy model
    - Threat Trees – Threat events
    - Threat graphs based on ATT&CK

Conduction

- ID threat sources relevant to organization
- ID threat events that could be produced by those sources
- IS vulnerabilities w/in the organization that can be exploited by threat sources
  → specific threat events and predisposing conditions
- Determine the likelihood that ID'd threat sources would initiate specific threat events + the likelihood the threat event would be successful
- Determine adverse impacts to organization's operations, assets, individuals, etc. from exploit
- Determine information security risks as a combination of
  → the likelihood of threat exploitation of vulnerabilities
  → the impact of the exploitation
  → any uncertainties associated with the risk determinations

Critical Assets:
Current:

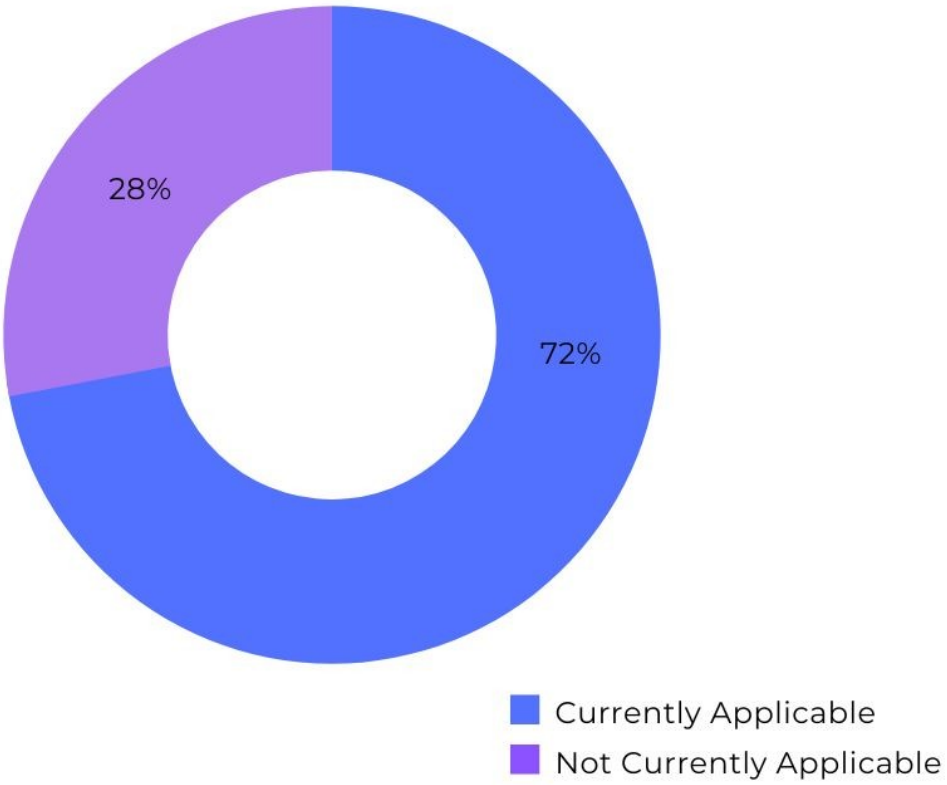
- Customer information
  - email communication
  - transaction log on software
- Supplier information
  - email communication
  - contact information
  - Supply contracts
- Warehouse
  - inventory list
    - ingredients
    - volume
  - delivery schedule
  - Personnel
- Tax/VAT information
  - sensitive customer information
    - credit card number, etc.
  - sensitive business information
    - tax ID, etc.
- Brick and Mortar
  - Face to face retail
  - customer transactions
  - Personnel
- Network and Tech
  - Storefront computer
    - Tax software
      - sensitive business information
        - tax ID, payments, etc.
    - Customer emails/details
      - pay by CC over phone?
  - Wifi router
    - mobile phones
  - LAN network
    - printers, fax machines
  - Warehouse computer
    - excel program
    - unpatched OS/browser

Digitization:

- web application
  - Administrative (private)
    - employee information
      - payment ID, etc.
    - supplier information
      - payment information, etc.
    - customer portal
      - payment information, etc.
  - customer portal (public)
    - usr/pwd, credit card, contact info
    - payment online
    - shopping cart
  - supplier portal (private)

        - usr/pwd, delivery schedule, contact information, product description, payment info
    - Warehouse portal
        -
    - employee portal (private)
        - user/psw, schedule, contact
    - Public portal (public)
        - Blog?
            - Allow comments?
        - Contact information
- Database (private)
    - Customer
        - transaction history
        - credit card information
        - contact information
    - Supplier
        - contracts
        - delivery log
        - product list
        - contact information
        - payment information
- Warehouse
    - Product supply
    - Product assembly
    - product deliveries
    - Personnel
- Brick and Mortar
    - Face to face retail
    - customer transactions
    - personnel
- Network and Tech
    - Storefront computer
        - see above
    - Warehouse computer
        - see above
    - wifi router
        - multiple connections
            - employee connection
            - storefront connection
            - warehouse connection
    - Firewall, VPN, Proxy
        - Use of third party product
            - Wix
            - Cloud
            - Amazon DB

ATTACKS APPLICABLE TO THE CURRENT ORGANIZATION STRUCTURE



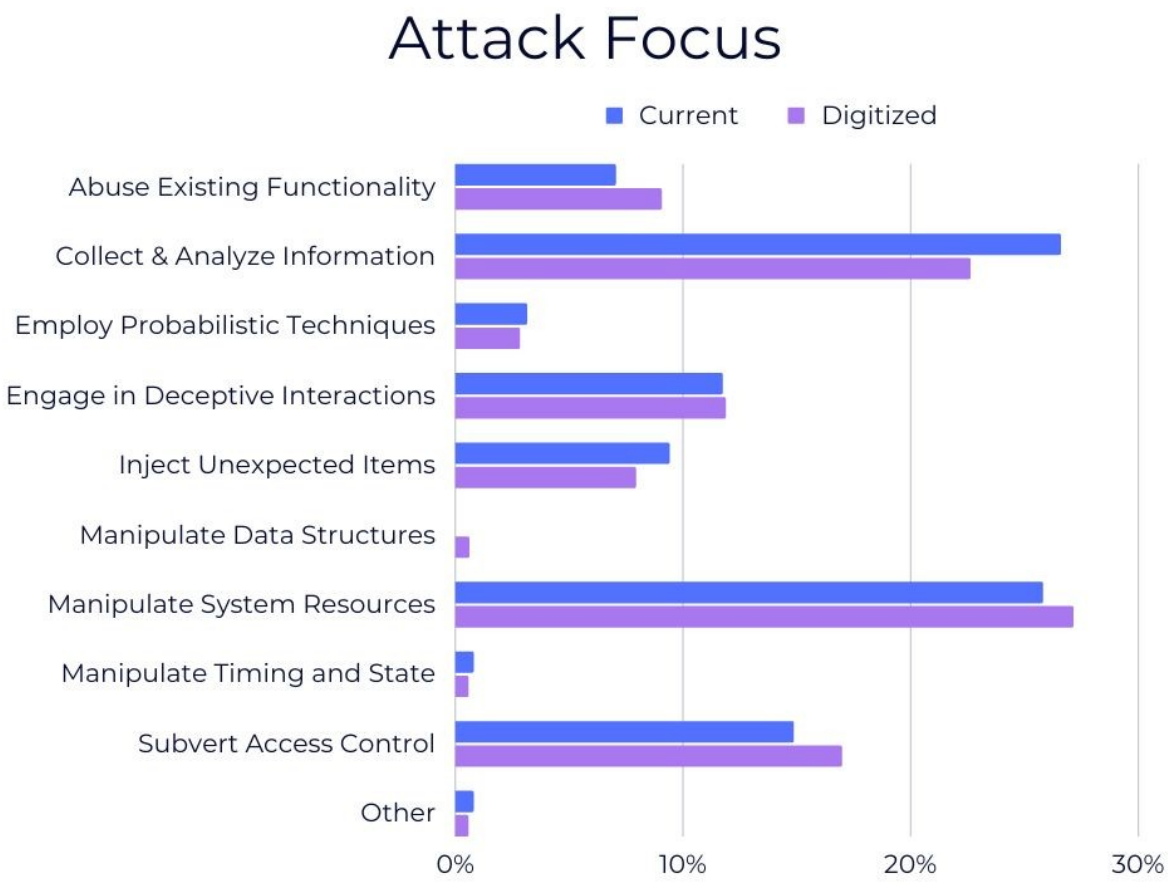


Table 1: Pampered Pets Attack Focus

Current Attack Focus	No. of Attacks	Total %	Digitized Attack Focus	No. of Attacks	Total %
Abuse Existing Functionality	9	7.03%	Abuse Existing Functionality	16	9.04%
Collect & Analyze Information	34	26.56%	Collect & Analyze Information	40	22.60%
Employ Probabilistic Techniques	4	3.13%	Employ Probabilistic Techniques	5	2.82%
Engage in Deceptive Interactions	15	11.72%	Engage in Deceptive Interactions	21	11.86%
Inject Unexpected Items	12	9.38%	Inject Unexpected Items	14	7.91%
Manipulate Data Structures	0	0.00%	Manipulate Data Structures	1	0.56%
Manipulate System Resources	33	25.78%	Manipulate System Resources	48	27.12%
Manipulate Timing and State	1	0.78%	Manipulate Timing and State	1	0.56%
Subvert Access Control	19	14.84%	Subvert Access Control	30	16.95%
Other	1	0.78%	Other	1	0.56%
Total No. of Attacks	128	100%	Total No. of Attacks	177	100%

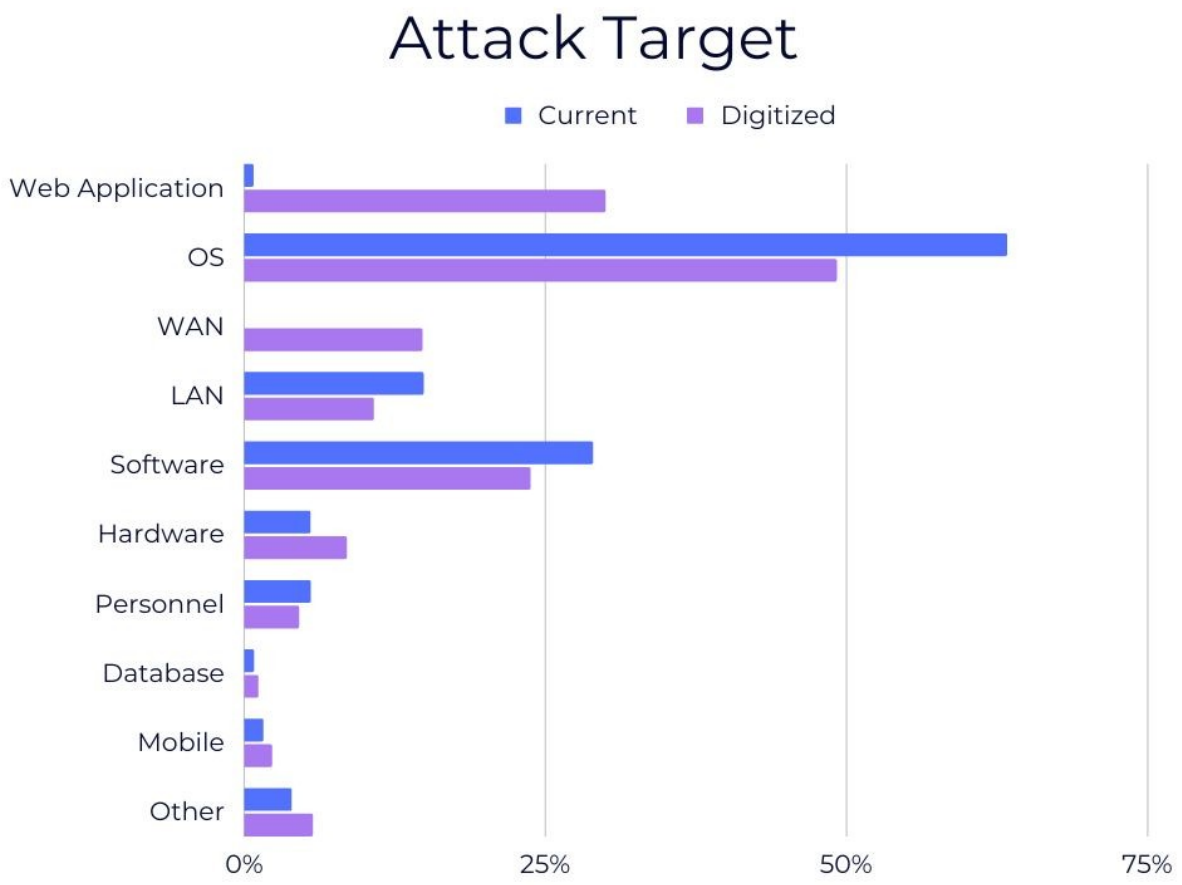


Table 2: Pampered Pets Attack Targets

Current Attack Targets	No. of Attacks	Total %	Digitized Attack Targets	No. of Attacks	Total %
Web Application	1	0.78%	Web Application	53	29.94%
OS	81	63.28%	OS	87	49.15%
WAN	0	0.00%	WAN	26	14.69%
LAN	19	14.84%	LAN	19	10.73%
Software	37	28.91%	Software	42	23.73%
Hardware	7	5.47%	Hardware	15	8.47%
Personnel	7	5.47%	Personnel	8	4.52%
Database	1	0.78%	Database	2	1.13%
Mobile	2	1.56%	Mobile	4	2.26%
Other	5	3.91%	Other	10	5.65%

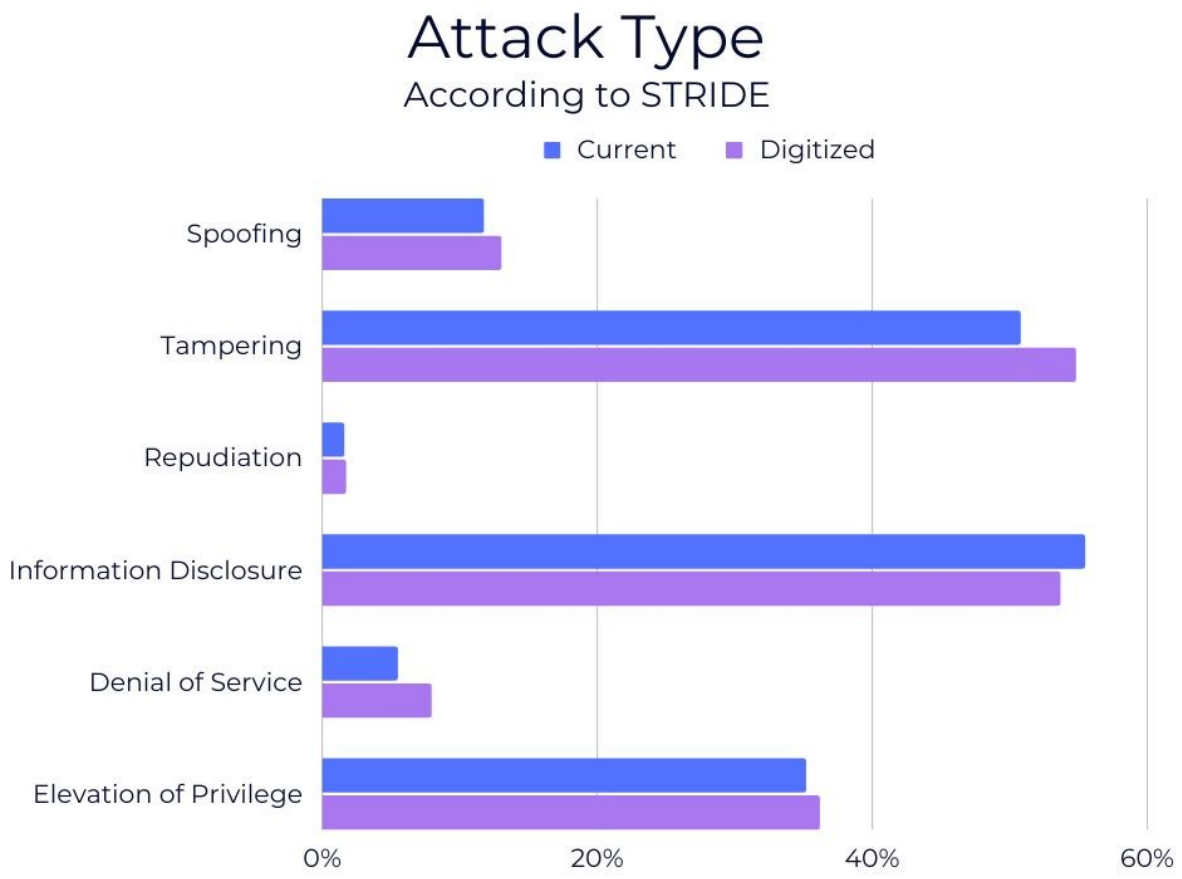


Table 3: Attacks by Type

Current Attacks by Type	No. of Attacks	Total %	Digitized Attack Targets	No. of Attacks	Total %
Spoofing	15	11.72%	Spoofing	23	12.99%
Tampering	65	50.78%	Tampering	97	54.80%
Repudiation	2	1.56%	Repudiation	3	1.69%
Information Disclosure	71	55.47%	Information Disclosure	95	53.67%
Denial of Service	7	5.47%	Denial of Service	14	7.91%
Elevation of Privilege	45	35.16%	Elevation of Privilege	64	36.16%

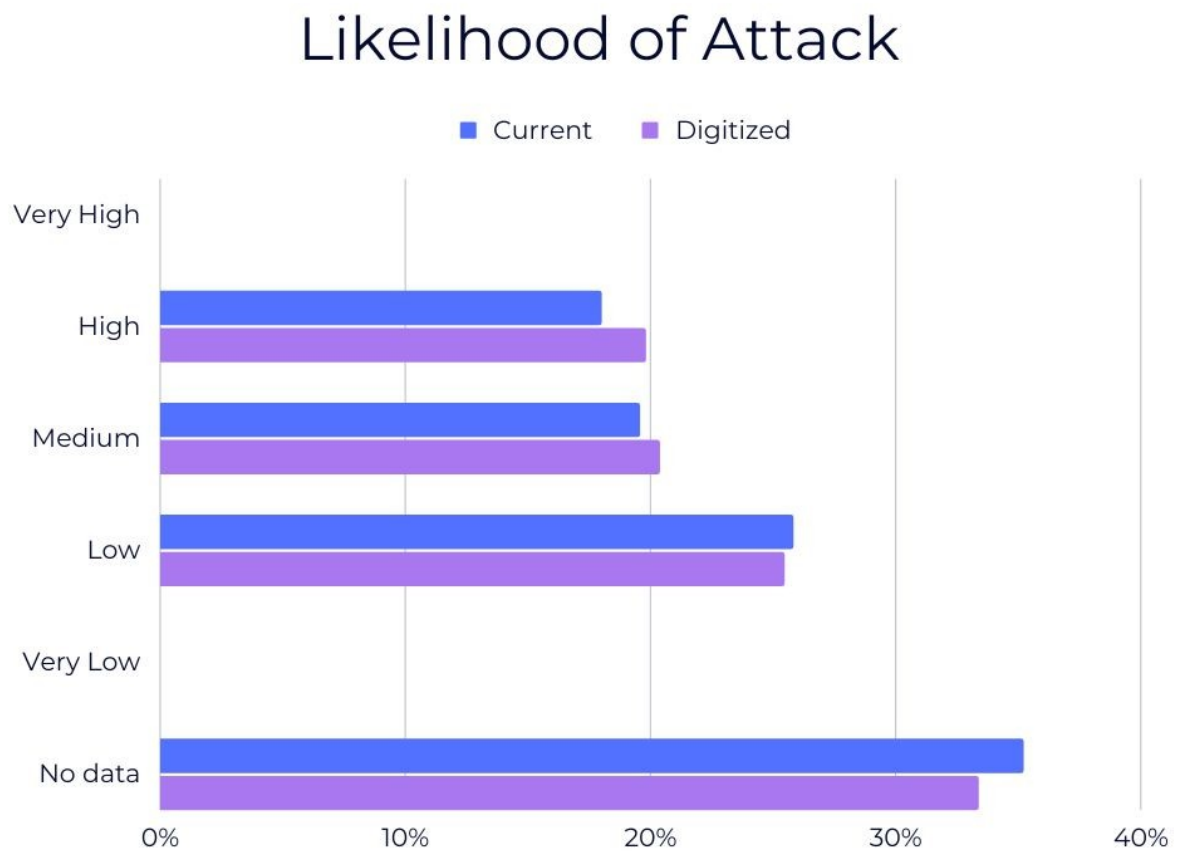


Table 4: Likelihood of Attack

Current Attack Likelihood	No. of Attacks	Total %	Digitized Attack Likelihood	No. of Attacks	Total %
Very High	0	0.00%	Very High	0	0.00%
High	23	17.97%	High	35	19.77%
Medium	25	19.53%	Medium	36	20.34%
Low	33	25.78%	Low	45	25.42%
Very Low	0	0.00%	Very Low	0	0.00%
n/a	45	35.16%	n/a	59	33.33%

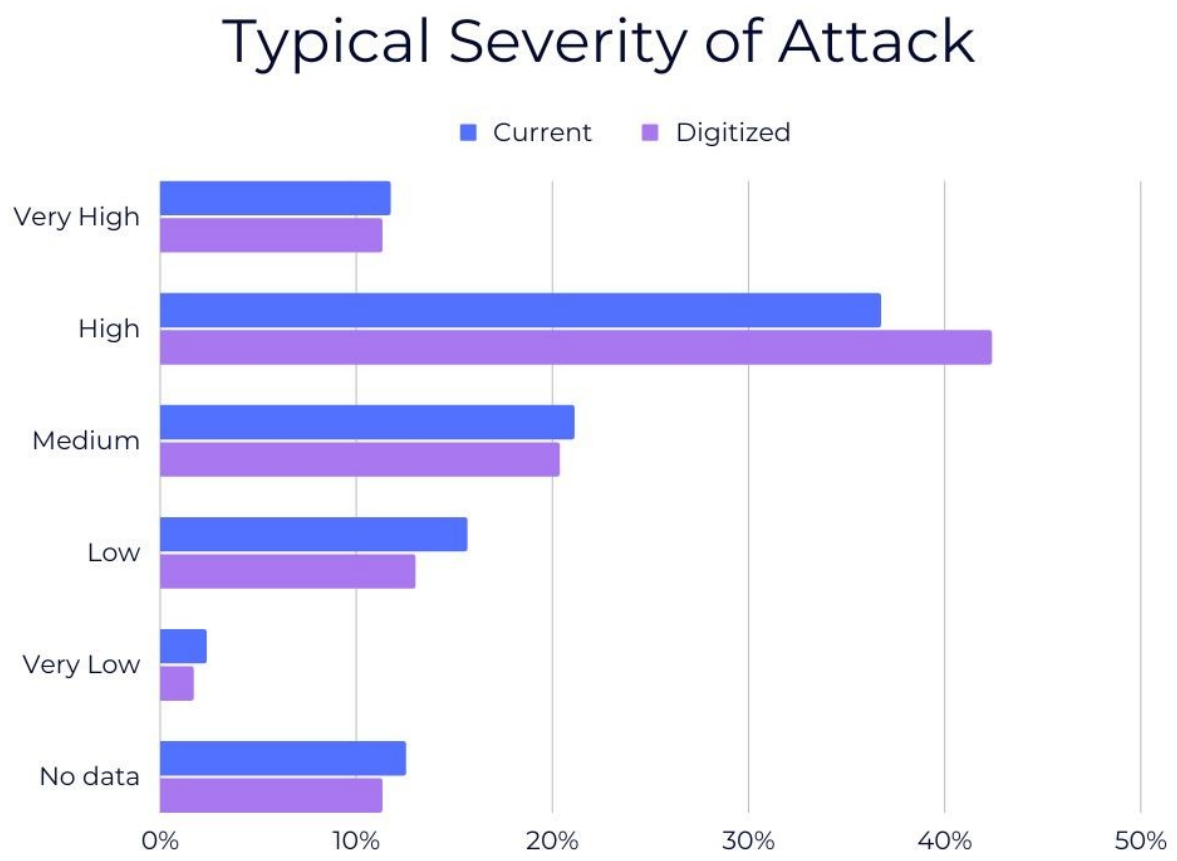


Table 5: Typical Severity of Attacks

Current Typical Severity	No. of Attacks	Total %	Digitized Typical Severity	No. of Attacks	Total %
Very High	15	11.72%	Very High	20	11.30%
High	47	36.72%	High	75	42.37%
Medium	27	21.09%	Medium	36	20.34%
Low	20	15.63%	Low	23	12.99%
Very Low	3	2.34%	Very Low	3	1.69%
n/a	16	12.50%	n/a	20	11.30%

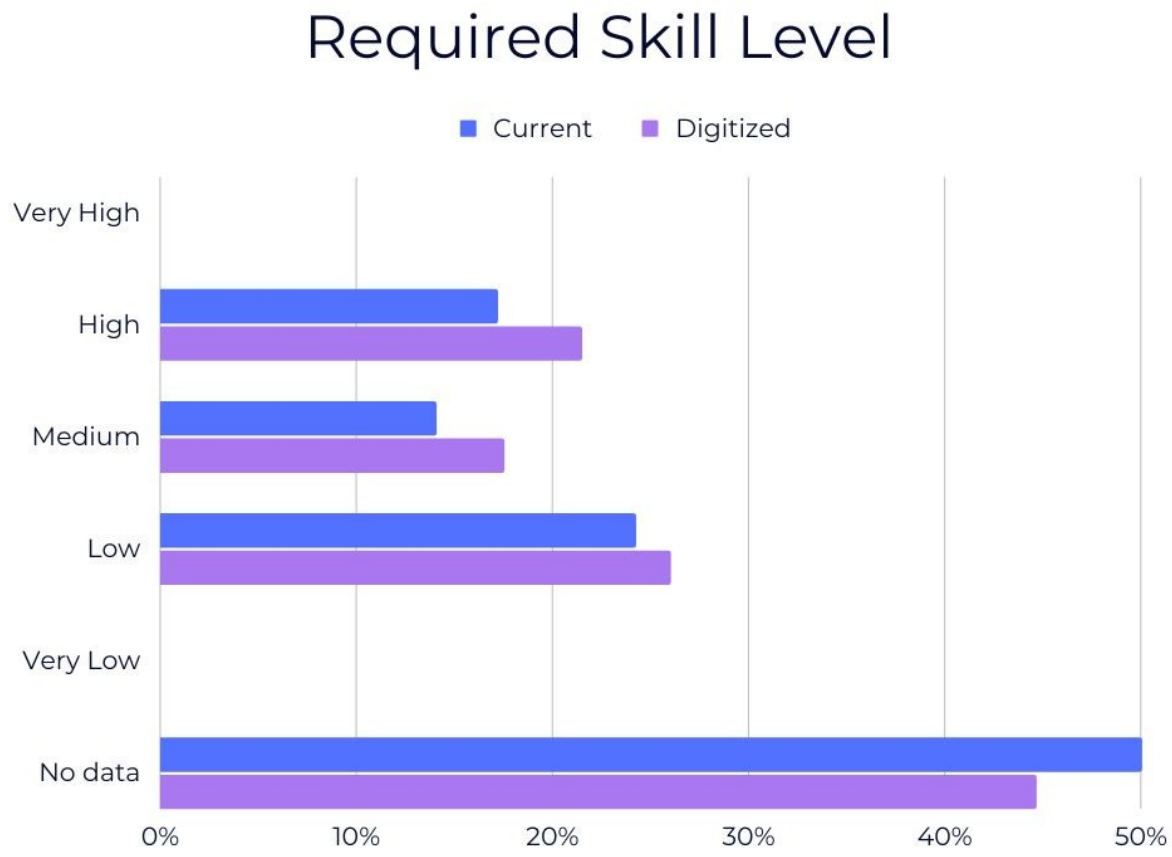


Table 6: Required Skill Level for Attack

Current Skill Level	No. of Attacks	Total %	Digitized Typical Severity	No. of Attacks	Total %
Very High	0	0.00%	Very High	0	0.00%
High	22	17.19%	High	38	21.47%
Medium	18	14.06%	Medium	31	17.51%
Low	31	24.22%	Low	46	25.99%
Very Low	0	0.00%	Very Low	0	0.00%
n/a	64	50.00%	n/a	79	44.63%

Table 7: Threat Profile of Current Threats

Attack Name	Likelihood of Attack	Typical Severity	Required Skill Level	Possible Mitigation(s)
Using Malicious Files	High	Very High	Low	Enforce principle of least privilege
Phishing	High	Very High	Medium	Employee training
Privilege Abuse	High	Medium	Low	Configure account privileges
Footprinting	High	Very Low	Low	Encrypt data, close unnecessary services/ports
Flooding	High	Medium	n/a	Configure limits of protocol scale

Table 8: Threat Profile of Digitized Threats

Attack Name	Likelihood of Attack	Typical Severity	Required Skill Level	Possible Mitigation(s)
Session Hijacking	High	Very High	Low	Encrypt identity tokens, session-key entropy
Adversary in the Middle	High	Very High	Medium	SSL/TSL encryption, public key security
Embedding Scripts within Scripts	High	High	Low	Input/output validation
Cache Poisoning	High	High	Medium	Disable client side caching
Repo Jacking	Medium	High	Low	Package management, lock files

Table: OCTAVE Impact Evaluation Criteria

Criteria	Low Impact	Medium Impact	High Impact
Customer Confidence	5% customer loss	10% customer loss	20% customer loss
Supplier Confidence	5% supplier loss	10% supplier loss	15% supplier loss
Financial	5% revenue loss	10% revenue loss	30% revenue loss
Legal	$10,000 lawsuit	$50,000 lawsuit	$100,000 lawsuit

Table: OCTAVE Information, Systems, and Applications

Systems	Applications	Information
Storefront Computer	Transaction software	Transaction documentation
		Tax and VAT information
	Email server	Customer contact/information
Warehouse Computer	Excel spreadsheets	Warehouse inventory
		Packing schedule
		Supplier delivery schedule
		Order fulfillment
		Storefront inventory
		Supplier information
	Email server	Supplier contact

Table: OCTAVE Critical Assets

Asset	Information Disclosure
Customer Information	Order records, contact information, payment methods
Supplier Information	Products, contact information, financial records, payment methods
Employee Information	Scheduling, contact information, financial records, payment methods
Transaction/Tax Information	Transaction records, tax/VAT records, financial records
Warehouse Inventory	Products, supplier delivery schedule, packing schedule

Table: OCTAVE System Problems (Attack Trees? p.524)

Possible Vulnerability	Customer Confidence	Supplier Confidence	Financial	Legal	Safety	Other
Software defects	H	H	H	L	L	--
System crashes	H	M	H	L	L	--
Hardware defects	M	M	H	L	L	--

Malicious code	H	H	H	M	M	--

Table: Other Problems

Possible Problems	Customer Confidence	Supplier Confidence	Financial	Legal	Safety	Other
Power supply	M	M	M	L	H	--
Telecommun-ications	H	H	M	L	L	--
Third Party	H	H	H	L	L	--
Natural Disasters	L	L	H	L	H	--

Table: Personnel Problems

Possible Problems	Customer Confidence	Supplier Confidence	Financial	Legal	Safety	Other
Key people taking a temp leave of absense	L	L	M	L	M	--
Key people leaving permanently	M	M	M	L	M	--
Threats affecting third party service provider	H	H	H	L	L	--

Table: OCTAVE Security Practices

Security Focus	Average Score	Security Competence
Security Awareness	1.2	Not at all
Security Strategy	1	Not at all
Security Management	1.13	Not at all
Collaborative Security Management	1.4	Not at all
Contingency Planning/Disaster Recovery	1	Not at all
Physical Access Control	2	Somewhat
Monitoring and Auditing Physical Security	1	Not at all
System and Network Management	1.1	Not at all
Monitoring and Auditing IT Security	1	Not at all
Authentication and Authorization	1	Not at all
Vulnerability Management	1	Not at all
Encryption	1	Not at all
Security Architecture Design	1	Not at all
Incident Management	1	Not at all
Total Score	1.2	Not at all

Table: OCTAVE Mitigation List

Mitigation		STRIDE Prevention	Example
In-House			
	Employee Training	S, R, E	Phishing prevention
	Security Strategy	T, I, D, E	Least Privilege Necessary policy
	Security Management	D, E	Clear implementation of security policy & regs
	Security Policy and Regulations	S, T, R, I, D, E	Clear outline of access controls, authentication strategies, and session management, and employee responsibilities
	Collective Security Management	S, R, E	Employee/manager input in security regulations
	Continued Planning	S, T, R, I, D, E	Continued risk assessment
	Physical Access Control	S, T, I	Warehouse access control
	Monitor Physical Sec	S, T, I	Security cameras in storefront and warehouse
	Authentication and Authorization	T, R, I, E	Username/password, employee ID
Third Party Vendor			
	System & Network Management	D	Enforcement of updated network protocols
	Monitor IT Security	T, I, E	Pentesting
	Authentication and Authorization	T, R, I, E	Access controls, two factor authentication
	Vulnerability Management	T, I, E	Software patching, pentesting
	Encryption	T, I	Hash 256
	Secure Architecture and Design	T, I, D, E	Have detailed explanation of system
	Incident Management	T, R, I, D, E	Have a security team to intercept/mitigate security breach