COVA CCI Cyber Internship Clinic Report:

Jendore LLC Cyber Risk Assessment Report

Team JenCyber

Mathieu Crosby, Jade Hines, and Wilondja Jacob

April 15th, 2025

CYSE 368: CyberClinic

Professor Teresa Duvall

Commonwealth
Cyber Initiative
COASTAL VIRGINIA

Table of Contents

I. Cybersecurity Clinic Background

The Old Dominion University Cyber Clinic is a 15 week program that allows students to receive real world experience by helping small businesses, non-profits, local government and other organizations around Hampton Roads. The intent of this program is to boost cybersecurity awareness and services to small businesses, such as JenDore LLC that may be in need of a cyber risk assessment. Team JenCyber have been equipped with knowledge in the National Institute of Standards in Technology (NIST) Cyber Risk Framework, design thinking, and tools for risk assessments on top of cybersecurity knowledge built up from their classes. Team JenCyber has been selected to create a tailored cybersecurity plan that addresses JenDore's concerns about cybersecurity risks to the business.

Our team consists of Jade Hines who is the team lead, Mathieu Crosby is the design lead, and Wilondia Jacob is the research/tech lead. The team lead is the main presenter, and facilitates communication internally and externally. The role of the design lead is to focus on the presentation elements, and is the forefront of prototypes and creation. The research/tech lead role of this person is to research companies and tech solutions, they are also to spearhead various tech initiatives as needed.

II. Overview of Retail

One of the largest and most dynamic industries in the world, retail includes a broad range of business models, such as direct-to-consumer brands, online platforms, subscription services, and brick and mortar stores. The business environment has changed dramatically in recent years due to the rise of e-commerce, with small businesses using digital platforms to compete in specialized sectors and satisfy particular client demands. Products that are personalized and custom-made have become increasingly popular as customers look for purchases that are more experience-driven, distinctive, and meaningful. Microbusinesses have emerged as a result of this change, and they succeed because of social media-driven marketing techniques and online stores.

JenDore LLC works in the subsector of gaming products and customized retail. This market niche targets customers that value practicality and individuality by combining aspects of handmade items, tech-related accessories, and creative design. The company sells branded items, clothing, gaming accessories, and personalized tumblers. The success of JenDore, a micro-sized e-commerce company, is mostly dependent on upholding a reliable online presence, efficient client interactions, and effective digital marketing initiatives. Additionally, cybersecurity is now crucial for maintaining company continuity and gaining the trust of customers due to the growth of peer-to-peer platforms and online purchasing.

This industry has unique cybersecurity risks since it relies significantly on digital tools for product development, online payment systems, and customer data collection. Small businesses, such as JenDore, are increasingly targeted by hackers because they are regarded to have weaker defenses than larger corporations. Phishing, financial fraud, and data breaches are all threats that can have a substantial impact on customer trust and business operations. As a

result, knowing the retail industry's digital risk landscape is critical for startups looking to assure long-term resilience and sustainable growth.

III. Threats Associated with Retail

The retail e-commerce industry, particularly small businesses like JenDore LLC, is vulnerable to a wide range of cybersecurity risks that can have a substantial impact on operations, customer trust, and financial stability. Understanding these dangers is critical for building effective safety mechanisms.

1. **Phishing and Business Email Compromise (BEC)**: Phishing attacks use fake emails or messages to deceive employees into disclosing confidential information or installing malware. BEC schemes especially target businesses by infiltrating official email accounts and conducting fraudulent transactions. According to the FBI's Internet Crime Complaint Center (IC3), BEC was one of the most expensive cyber threats, with 21,489 reports resulting in damages over $2.9 billion in 2023. A successful BEC attack on a small e-commerce business like JenDore could result in unlawful fund transfers or the exposure of client data, jeopardizing financial health and customer confidence.

2. **Ransomware Attacks:** Ransomware is malicious software that encrypts a company's data and makes it unavailable unless a ransom is paid. In 2023, IC3 received over 2,825 ransomware complaints, up 18% from the previous year, with total losses jumping 74% to $59.6 million. Small retailers are frequently targeted due to perceived inadequate security measures. An attack on JenDore might disrupt operations, cause data loss, and result in considerable recovery expenses, emphasizing the importance of effective data backup and incident response policies.

3. **Data Breach and Credential Harvesting:** Cybercriminals regularly create counterfeit login pages that seem like authentic brand websites to steal user credentials. These "scampages" trick customers into supplying login information, which is subsequently used to fraudulently access accounts. The FBI has seen an increase in such approaches, with fraudsters selling these tools to others, increasing the threat. For JenDore, a data breach that compromises client credentials could result in illegal account access, financial fraud, and reputational damage.

4. **Supply Chain Vulnerabilities:** Many small e-commerce businesses rely on third-party contractors to handle payment processing and order fulfillment. Cyberattacks on these service providers have the potential to have an indirect impact on merchants. For example, a ransomware attack on a supply chain management software company impacted operations for several stores, demonstrating the cascading effect of similar occurrences. JenDore's reliance on external partners needs extensive assessment and ongoing monitoring of their cybersecurity policies to mitigate supply chain threats.

5. **Automated Bot Attacks:** According to Axios, retail websites experienced an alarming increase in AI-driven bot attacks in 2024, with over 560,000 automated attacks per day between April and September. These bots are used for credential stuffing, inventory scraping, and even fraudulent purchases. Such attacks may overload JenDore's online infrastructure or compromise important information, making anti-bot defenses critical to long-term security (Axios, 2024).

Addressing these cybersecurity threats necessitates a complete strategy that includes employee training, strong security policies, regular system audits, and collaboration with cybersecurity professionals. By proactively recognizing and addressing these risks, JenDore can protect its operations, customer data, and brand trust.

IV. Jendore

IVa. Company Description

JenDore LLC is a small, woman-owned retail business located in Portsmouth, Virginia that specializes in handmade items, personalized gifts, and gaming accessories. JenDore appeals to customers that want unique and customized items. As a startup with a small number of employees, the company primarily works through its e-commerce platform, which offers a variety of handmade and tech-related goods. JenDore's digital storefront and social media presence are its key platforms for product sales, customer engagement, and brand promotion.

IVb. History

JenDore LLC was founded by entrepreneur Jena Green, who had a passion for design, crafting, and creativity. Initially a side project, the company grew into a full-fledged business offering a diverse range of customized products, including tumblers, shirts, gaming gear, and computer accessories. The ambition to produce high-quality, unique things with a personal touch has been the driving force behind the brand's continuous growth and dedicated fanbase.

JenDore, based in the Hampton Roads region, has built a reputation for rapid customer service, a community-oriented approach, and strong online involvement. JenDore, a private, for-profit startup, is expanding its presence in both local and digital marketplaces, with long-term goals of improving cybersecurity, operational continuity, and regulatory compliance.

IVc. Social Media Presence

JenDore has a strong presence on several social media sites, including Instagram, Facebook, and TikTok. These channels are largely used for marketing, introducing new products, interacting with customers, and increasing traffic to their online store. To increase community

involvement, the company makes excellent use of visually appealing material, trending music, and interactive posts.

From a cybersecurity point of view, however, the company's extensive social media presence also presents potential threats including impersonation, phishing, and platform-specific vulnerabilities. Their visibility raises the risk of data leaking via third-party app integrations or corporate email compromise (BEC). It is essential that JenDore implement best practices for protecting social media accounts, such as frequent password changes, two-factor authentication (2FA), and awareness of social engineering techniques. By reinforcing these areas, risks connected to digital operations that are visible to the public will be reduced.

The main website can be found at the URL https://www.jendore.com and works as an online store front. The website also links to Facebook, Instagram, TikTok, X (Twitter) and Pinterest. The website provides a way to contact through the website's live chat which has been done through shopify. The store page on the website also gives in person shop locations to buy JenDore products as well as a pop up shop with location and time. This website also sends people to a door dash site to buy JenDore products.

The Facebook with the link https://www.facebook.com/jendorestore has 55 followers and the Facebook account links to the website, Instagram, Pinterest, TikTok and X. This account gives the address of the pop up shop, a phone number (+1 (757) 204-1424) and a support email address (support@jendore.com). This email was then run through an email checker to see if the email has been involved in a data breach (https://haveibeenpwned.com/). This email has not been involved in any cyber breach. The Facebook includes posts about the pop up at Selden Market and the Twitch account.

The JenDore Twitch account can be found at https://www.twitch.tv/jendore there appears to be zero current followers and it links the Facebook account and the Instagram account. The live streaming recordings do not appear to persist after the live event. The last known stream was March 14th, as Twitch will say how long ago the last stream was. The last known stream according to Facebook and Instagram posts are Fortnite streams.

The Instagram account can be found at https://instagram.com/jendorestore and has 181 followers. This Instagram account links to the JenDore store, TikTok, the Bloom Market Facebook, and Twitch. This social media profile also connects to the Instagram Threads which is another way to post about going live on Twitch. Instagram also has a direct messaging option that works as a business chat that has an automatic response messaging system. The business chat could be another way to redirect users to a different mode of communication or preferred method of contact.

The TikTok that is found at the URL https://www.tiktok.com/@jendorestore would be good for marketing outside of the United States for international customers. The TikTok account has 25 followers and the amount of views tend to range from 500 to 1500 per video. I think it would be good to market the new items in the online store considering the state of TikTok in the United States over the opening times for the pop up shop. This account is also linked to the JenDore Store and has the username handles of the Facebook account and the Instagram account.

Pinterest can be found at https://pinterest.com/jendorestore and has five followers, this account can be linked back to the online store and the instagram account. This Pintrests page is also a verified merchant account. The posts also link to the PoshMark where people can also buy things under that account for the JenDore Store. The PoshMark account is a Posh Ambassador that can be found at https://poshmark.com/closet/jendorestore and as of March 31st, 2025 has

726 listings, 5,597 shares, and 61,399 followers. This store also links to the original JenDore site. There might be a slight disconnect between the main site and the offbranch on PoshMark as the coasters are 99 cents cheaper and there are some items that appear to be sold out on the main site that are available on PoshMark.

The Twitter can be found at the URL https://twitter.com/jendorestore and has 52 followers, links to the JenDore store. This social account also has not shown activity since November 8th, 2024. This site also requires premium or paid Twitter in order to privately message JenDore. The Twitter account does link to a Mercari account which can be found at https://www.mercari.com/u/jendore/? with 2858 reviews, being known for quick shipping, item descriptions and packaging. This Mercari profile has a listing of 240 items, with 181 of those items being for sale and having sold 2934 items. This profile also has a following of 1445 people.

The Bluesky account has been a recent addition to all the other social media accounts as of 2 months ago. The Bluesky account can be found at the handle @jendorestore.bsky.social and URL https://bsky.app/profile/jendorestore.bsky.social with a following of 3 people and 5 posts. The account does not link up to anything but the posts have the JenDore store link in them for people to follow.

V. Risk Assessment

Valor Cybersecurity was one of our primary partners for the Cyber Clinic. The Valor's Top Ten Checklist is one of the resources they made available to us. Valor's Top Ten Checklist is a set of cybersafe practices that every business should strive for to have a good baseline of security. Although our clinic review with Valor's Top Ten Checklist addresses only the first seven evaluative areas, Team JenDore reviewed and addressed all ten.

1. Annual Digital Risk Checkup

An annual evaluation of digital vulnerabilities would be conducted to examine potential advantages and disadvantages. This would be a list of the digital assets, potential risks to each, and whether backups or safeguards are in place. The digital risk check up has not been implemented yet. Having a list of all the various systems in use, including payment, social networking, and inventory management would be the best method to accomplish a digital risk check up. In identifying all digital assets it helps identify all digital risks because in itemizing everything it helps show what is already in place for protection of other digital assets.

2. Access Check and Minimal Permissions

The purpose of an access check is to restrict who has access to important information and systems. Although JenDore is now managed by a single individual, other individuals can access the accounts in case the primary employee has a health issue. An access control list that identifies who has access in an emergency should be in place. Plans for the bare minimum of authorization required for future potential jobs to effectively perform their duties should likewise be in place.

3. Backup Data and Software, then Test

Regularly backing up your data is essential for business continuity. It is equally important to test those backups to ensure they are functioning correctly and fully restorable in the event of a cyber incident. A good standard to follow is the **3-2-1 rule**: keep **three** different copies of your data, on **two** different storage types, with **one** copy stored off-site.

JenDore currently uses both external hard drives and cloud storage for backups and performs occasional testing, which is a great foundation. To strengthen this practice, we recommend creating a formal backup policy that defines how frequently both the cloud and physical backups should be updated and tested.

4. Double Layer Protection Shield

Multi-factor authentication (MFA) offers an important second layer of protection by requiring both a password (something you know) and a code transmitted to your device (something you have). Requiring these factors dramatically minimizes the likelihood of unwanted access to critical company accounts.

JenDore has already introduced MFA for specific accounts, which is a great start. We advocate broadening this security to include all admin-level, email, and payment systems, resulting in a more consistent shield across platforms.

5. Digital Perimeter Guard

A firewall serves as a digital perimeter, filtering incoming and outgoing traffic to secure your company's internal systems. while used in conjunction with a Virtual Private Network (VPN), these solutions help to secure sensitive data, particularly while accessing workplace resources remotely.

JenDore does not currently utilize a VPN for business activity. We recommend getting one, especially for remote work circumstances or mobile access to customer data. Strengthening the digital perimeter will help protect critical business assets from unauthorized access.

6. Draft a Digital Playbook

A digital playbook provides a clear blueprint for protecting digital assets. It should help anyone who reads it understand what steps to take in the event of a cyberattack or security issue. JenDore is currently developing this resource and already has a simplified version available for others to use in case of an unexpected incident or disruption.

7. Employee Bootcamp

Employee boot camp includes training all personnel with cyber awareness so that they could safely navigate the networks. Currently, there is only one employee. However, new staff should receive a brief training and knowledge before being granted access to the system. Training should include understanding social engineering attacks, strong passwords, and how to use current technologies safely.

8. Digital Personnel Management

Digital Personnel Management is an important aspect of access control. It ensures that new employees are granted appropriate access after completing onboarding, and that former employees no longer retain access to company systems. While digital personnel management is not currently a concern at JenDore due to its single-user setup, it will become increasingly important as the team grows. Implementing an access control list in the future will help define who has access to what, based on their role and responsibilities.

9. Digital Surveillance

Digital Surveillance involves actively monitoring both digital and physical systems to detect suspicious activity and prevent security breaches. Digitally, surveillance could include an Intrusion Detection System (IDS) that monitors for attempted attacks and confirms whether they are blocked by the firewall. Physical surveillance, such as security cameras, helps ensure that only authorized individuals access equipment and facilities. It also plays a key role in identifying any tampering with physical systems.

10. Fortify your Digital Mailbox

Fortify Your Digital Mailbox by enhancing the security of your email system to defend against common threats like phishing and spam. At present, JenDore relies on Gmail's built-in filtering system, which primarily targets spam. While the built in filters provides a basic layer of protection, it does not consistently catch phishing attempts or distinguish between promotional emails and legitimate requests for customized content. Exploring additional email security tools or third-party filters could strengthen this area and reduce exposure to email-based threats.

VI. Assets, Risks, and Controls

1. Assets (Identify Function – NIST)

JenDore's critical digital and physical assets include:

- **E-commerce Website**: www.jendore.com – main sales and marketing channel
- **Customer Data**: Email addresses, shipping/billing information, and purchase history
- **Business Email Accounts**: Used for customer communication, vendor relations, and order processing
- **Point-of-Sale & Payment Processing Systems**: Likely integrated with Stripe, PayPal, or Shopify
- **Social Media Accounts**: Instagram, Facebook, and TikTok used for marketing and customer engagement
- **Computers & Mobile Devices**: Used for managing the business, creating content, and customer service

2. Risks (Assess and Analyze – NIST Risk Management Framework)

Each asset presents potential risks:

- **Website**: Susceptible to hacking, malware injection, denial-of-service attacks
- **Customer Data**: Risk of data breach or theft, especially if unencrypted or inadequately protected
- **Email Accounts**: Vulnerable to phishing and Business Email Compromise (BEC)
- **Payment Systems**: Target for financial fraud, especially if compliance measures (like PCI-DSS) are not followed
- **Social Media**: Risk of impersonation, account hijacking, or reputational damage

- **Devices**: Could be infected with malware or ransomware if security updates are not maintained

3. Controls (Safeguards – Protect & Detect – NIST) / Implementation Suggestions

Category	Risk Control	Description
Access Control	Use Multi-Factor Authentication (MFA)	Implement MFA for all email, website admin, and payment portals
Data Protection	Regular Encrypted Backups	Automate backups of customer data and website to a secure, encrypted drive or cloud
Awareness Training	Social Engineering & Phishing Training	Train business owner/team to recognize and respond to phishing scams and suspicious emails
System Security	Device and Software Updates	Keep all business devices and plugins/software updated to patch vulnerabilities
Vendor Risk Management	Review Third-Party Services	Ensure vendors (e.g., website host, payment processors) comply with cybersecurity standards
Incident Response	Create a Simple IRP	Establish a short, clear incident response plan with key contacts and steps to isolate, report, and recover
Monitoring	Use Activity Logs & Alerts	Monitor login activity and failed attempts on website admin panel and email accounts
Website Security	Enable HTTPS and Web Application Firewall (WAF)	Use SSL certificates and host platforms that provide basic web application security features

VII. Specific Questions from JenDore

The following questions were submitted by JenDore, LLC in their application, highlighting the specific cybersecurity topics they are most interested in exploring to better protect their business.

How do I implement basic cyber risk management practices?

Implementing basic cyber risk management starts with identifying and categorizing your business assets such as your website, customer data, payment platforms, and devices. Once you know what needs protecting, assess what threats (like data breaches or email compromise) could affect them. Based on this, prioritize protections such as:

- Using strong, unique passwords and enabling multi-factor authentication (MFA)
- Keeping devices and software updated
- Backing up data regularly to a secure, offline location
- Limiting user access to only what's necessary for their roles

A simple written cybersecurity policy and a regular review of these practices can help ensure ongoing protection.

How do I create a cybersecurity incident response plan?

A cybersecurity incident response plan (IRP) outlines how your business prepares for, detects, contains, and recovers from cyberattacks. It should include:

- **Preparation:** Identify a response team (even if it's just the business owner or a trusted IT partner)
- **Detection:** Define what qualifies as an incident (e.g., unauthorized login, ransomware alert)

- **Response:** Steps to isolate affected systems, secure data, and stop the attack
- **Recovery:** Restore from backups and test systems before going live again
- **Post-incident:** Document the event, evaluate the response, and update procedures

  For a business like JenDore, this plan should be short, practical, and printed or saved securely for quick access.

How do I respond to cyber attacks and who do I report them to?

If you experience a cyberattack:

- Disconnect affected systems from the internet immediately to contain the threat.
- Notify your web host, IT support, or managed service provider if available.
- Use your incident response plan to begin recovery.
- Change passwords and monitor accounts for suspicious activity.

You should report cyber incidents to:

- **FBI Internet Crime Complaint Center (IC3):** https://www.ic3.gov
- **CISA (Cybersecurity & Infrastructure Security Agency):** https://www.cisa.gov/report
- **Local law enforcement** (especially if fraud or data theft is involved)

  Reporting helps law enforcement track trends and potentially assist in recovery or legal protection.

How do I implement cybersecurity best practices?

Cybersecurity best practices for a small retail business like JenDore include:

- Using reputable e-commerce platforms with built-in security features
- Regularly updating plugins, themes, and software used on the website
- Encrypting customer data and payment transactions
- Training all staff (even if it's just the business owner) on phishing and social engineering

- Implementing website monitoring tools and firewalls

Also, perform periodic reviews of vendor security and create a checklist for evaluating any third-party services you use.

VIII. JenDore Original Application Requests

Based on JenDore LLC's application, the company operates in the **retail sector** as a **private, for-profit startup** with **1–10 employees**. Their primary **cybersecurity concerns** include:

- **Data breaches**
- **Business email compromise**
- **Compliance with data protection regulations**
- **Vendor/third-party cybersecurity risks**

They also indicated strong interest in:

- Implementing **basic cyber risk management practices**
- Developing a **cybersecurity incident response plan**
- Learning how to **respond to attacks and where to report them**
- Following **cybersecurity best practices**

In alignment with their **2–3 year cybersecurity goals**, we recommend the following targeted next steps:

- **Establish a simple written cybersecurity policy**, tailored to JenDore's size and structure
- **Create a one-page IRP** and test it annually through a mock exercise
- **Set up secure backups** using encrypted cloud or offline storage solutions
- **Enable MFA** across email, website admin, and payment platforms

- **Vet third-party vendors** using a checklist of basic cybersecurity controls (e.g., encryption, compliance certifications)
- **Enroll in free webinars** and workshops hosted by organizations like CISA, NIST, or COVA CCI to stay updated

With these measures in place, JenDore will be positioned to proactively manage cyber risk and protect its growing digital business.

IX. Overall Conclusion

SWOT Analysis

A SWOT analysis is a strategic planning tool used to identify and evaluate the **Strengths, Weaknesses, Opportunities,** and **Threats** related to a business or project.

- **Strengths** are internal advantages that give the business a competitive edge.
- **Weaknesses** are internal areas that may hinder growth or performance.
- **Opportunities** are external factors that the business can take advantage of for growth.
- **Threats** are external challenges that could negatively impact the business.

In the context of cybersecurity, a SWOT analysis helps a business like JenDore better understand its current security posture and prioritize areas for improvement and investment.

Strengths	**Weaknesses**
• Strong online presence across website and social media platforms • Engaged customer base and growing brand identity • Willingness to learn and adopt cybersecurity best practices (as indicated in the application)	• No current written cybersecurity policy or incident response plan • Limited cybersecurity training or dedicated IT staff • Reliance on third-party vendors for key services like payments and hosting, increasing external risks
Opportunities	**Threats**
• Access to free cybersecurity resources, training, and consultation through programs like COVA CCI • Implementing low-cost tools like multi-factor authentication, encrypted backups, and free antivirus/firewall tools • Increasing consumer trust by promoting secure checkout, privacy policies, and response readiness	• Business Email Compromise, ransomware, and phishing attacks targeting small businesses • Supply chain vulnerabilities from third-party services with weak security • Social media account hijacking or brand impersonation

Best Bang for Their Dollar: Recommendations

Given JenDore's size and business model, our team recommends the following low-cost, high-impact actions that provide the **best return on investment (ROI)**:

1. **Enable Multi-Factor Authentication (MFA) Across All Accounts**

   Free to implement; dramatically reduces risk of email compromise and unauthorized access.

2. **Create and Print a 1-Page Cybersecurity Incident Response Plan**

   Simple, practical, and can be built using templates. Prepares the business for any type of incident, from phishing to ransomware.

3. **Use Free or Built-in Website Security Features**

   Ensure the site uses HTTPS, enable spam/malware filters, and regularly review admin logins.

4. **Perform Weekly Encrypted Backups to External Storage or Cloud**

   Inexpensive and vital for ransomware recovery and data loss prevention.

5. **Complete One Staff Cybersecurity Awareness Training Session per Quarter**

   Use free resources from the FTC, CISA, or NIST. Even a short 15-minute session can significantly reduce human error.

Final Thoughts

JenDore LLC is a promising and passionate small business with a developing online presence. As the company's online presence grows, cybersecurity must be viewed not as a technical challenge, but as an essential component of business resiliency and customer trust. The steps listed above are cost-effective, scalable, and practical. It ensures JenDore's expansion is secured against emerging digital threats.

X. Applicable References

Gmail offers built-in filtering tools that can help organize and manage incoming messages by automatically detecting potential spam or routing emails to designated folders. To better support business operations, JenDore can create **custom filters** based on how each email address is used.

For example, emails sent to **support@jendore.com** containing keywords like *"custom product request"* could be automatically directed to a dedicated folder for custom orders. Implementing this type of filtering strategy can help streamline communication and reduce clutter, offering an effective first step before investing in third-party email or spam filtering tools. https://www.youtube.com/watch?v=S9Uhr7RhyiM

These are a few links that lead to the advice of the Cybersecurity and Infrastructure Security Agency. These links include some actions that the business can take when it begins to incorporate more people. These links also look at general performance goals in the case of creating an incident response plan focused around the National Institute of Standards in Technology's Cyber Risk Management framework. They look into different possible ways to identify risks, protect against them, detect, properly respond and recover from possible attacks.

General Guidance for Business Growth: https://www.cisa.gov/cyber-guidance-small-businesses

Risk Management Framework: https://www.cisa.gov/cybersecurity-performance-goals-cpgs

Email Specific Protection:
https://www.cisa.gov/news-events/directives/bod-18-01-enhance-email-and-web-security

Phishing Awareness Training:
https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

The Federal Trade Commission has an assortment of different models for information to help inform small businesses more about how they can better protect themselves.

FTC: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

The Department of Defense offers a robust cyber security training course which can help with creating employee training courses. These trainings seem to be updated yearly to account for the difference in year.

DoD Training courses: https://public.cyber.mil/cyber-training/training-catalog/

XI. Future

To assist JenDore LLC develop in cybersecurity, our team recommends building a cyber hygiene training program and creating a basic, actionable **Incident Response Plan (IRP)**. These activities will strengthen long-term resilience and assistance in the prevention or effective response to possible cyber incidents.

Cyber Hygiene & Best Practices Training

Cyber hygiene refers to a set of routine practices and habits that ensure the safe handling of data and systems. For JenDore, this training can be provided quarterly in brief, easy-to-understand sessions, covering:

- **Phishing Awareness** – How to spot suspicious emails, links, and fake login pages.
- **Password Management** – Use of strong, unique passwords and password managers.
- **Multi-Factor Authentication (MFA)** – Why and how to activate MFA on all critical accounts.
- **Device Security** – Keeping operating systems, browsers, and software updated.

- **Safe Social Media Usage** – Preventing impersonation, hijacking, or oversharing sensitive info.
- **Secure Backups** – Ensuring encrypted and regular backups are performed (cloud or external drive).
- **Safe Use of Public Wi-Fi** – Recommendations to avoid accessing sensitive accounts on unsecured networks.

Useful free resources for this training include:

- FTC Cybersecurity for Small Businesses
- CISA Cyber Essentials
- National Cybersecurity Alliance

Incident Response Plan (IRP) – Government Contacts & Next Steps

An IRP is essential to prepare for unexpected cybersecurity incidents. JenDore should develop a simple, one-page plan that includes:

- **Incident Identification** (e.g., phishing, malware, website defacement)
- **Immediate Response Steps** (disconnect device, notify email provider, change passwords)
- **Recovery Steps** (restore data from backup, scan systems, notify customers if needed)
- **Documentation** (record timeline of incident and recovery)
- **Post-Incident Review** (analyze what went wrong and update protections)

Recommended Government Contacts in Case of a Cyber Incident:

Agency	Purpose	How to Report
FBI – Internet Crime Complaint Center (IC3)	Report cyber fraud, business email compromise, ransomware	https://www.ic3.gov
CISA (Cybersecurity & Infrastructure Security Agency)	Report critical infrastructure attacks, receive technical assistance	https://www.cisa.gov/report
Local FBI Field Office – Norfolk, VA	For serious cybersecurity incidents requiring immediate law enforcement support	Phone: (757) 455-0100

JenDore LLC can dramatically limit its exposure to cyber threats and respond effectively to incidents by proactively conducting cyber hygiene training and developing an IRP. As a growing small firm, investing in these core principles provides significant benefit at a cheap cost, promoting both stability and long-term success.

While this assessment offers fundamental suggestions suitable for JenDore LLC's current size and operations, it is critical to understand that cybersecurity is a continuous activity. As the company develops its digital presence or adopts new technology, additional work will be required to analyze risks, update security policies, and install more complex measures. Continued engagement with cybersecurity professionals, frequent training, and a yearly review of the incident response strategy will ensure JenDore's resilience in an ever-changing threat landscape.