Cybersecurity Fundamentals Exercise

Members: Debojyoti Mishra
Tien Quoc Bui
Natthanicha Vongjarit
Phuong Khanh Pham

Problem: Your company is a newly growing start-up in the SaaS industry with an on-premises data center located in the Caribbean and a headquarters in Paris. You are hiring new personnel and your customers are located in eastern Europe. Your product was fielded quickly in order to seize an opportunity due to changes in the local economy you want to capitalize on before your competition breaks into the market. What are the risks to your business, how will they impact your business and how will you recover and restore service when things fail.

Slide: click here
Mathew.davis1@fulltiltcyber.com

I. Introduction:

Company:

Goal: We develop Inventory and Supply Chain Management Tools designed to support the growth of newly emerging companies in our target country, driven by the benefits of an improving economy.

Examples of SaaS companies providing Inventory and Supply Chain Management: SAP Ariba, Oracle Netsuite.

Welcome to our presentation on the key risks our startup faces and how we can overcome them. We'll explore challenges like geographic risks, customer service issues, and the impact of emerging technologies. We'll also discuss practical *solutions, such as scalable infrastructure, cybersecurity, and customer-focused strategies, to ensure long-term success in the competitive SaaS market.*

Product: Inventory and Supply Chain Management Tool

II. **Risks:**

1, Data Breach

a. **Explanation:**

   i. Data breaches can occur due to various reasons such as weak access controls, unpatched software vulnerabilities, insider threats, or external attacks like APTs and hackers. These breaches may expose sensitive customer data, lead to the theft of intellectual property, or may include employee personal information which lead to putting employees in risk.

Moving on to the impact of data breach. I'm sure that the impact of this are infinity but in term of company lets divided in 3 general impact

b. **Impact:**

   i. A data breach can significantly damage your **reputation**. In the B2B Saas industry, trust is crucial, and a breach could lead to immediate customer churn, making 3-7% of customers leave right away and new customers might extend sales cycles by 30-60 days. It also attracted negative media attention both locally and internationally, increasing scrutiny from analysts and investors. Recovering your reputation could take 1-2 years.

   ii. **Competitively**, a breach can erode your advantage if proprietary algorithms are compromised, potentially giving competitors the opportunity to replicate your unique features. This could result in a 6-12 month loss of competitive edge and a 5-15% market share decline within six months. Additionally, resources diverted to manage the breach could delay product development by 3-6 months, giving competitors a chance to catch up.

   iii. **Financially,** the costs can be extensive. Direct expenses might include investigation and forensics, notification of affected individuals, credit monitoring services, and potential regulatory fines, which can reach up to €20 million or 4% of global turnover under GDPR since we are based in europe. Indirect costs may involve a 20-30% revenue decline in the first year, potential class-action lawsuits, and a significant increase in cybersecurity insurance premiums.

c. **Remediation:**

- Data Encryption:
  - Implement strong end-to-end encryption for sensitive data, both in transit and at rest, and manage encryption keys securely.
- Cyber Insurance:
  - Obtain comprehensive cyber insurance and regularly review and update your coverage to address evolving risks. Ensure you understand the policy requirements for incident response.
- Incident Response Planning:
  - Develop and regularly test an incident response plan, establish a dedicated incident response team, and create communication templates for various breach scenarios.
- Third-Party Risk Management:
  - Conduct thorough security assessments of vendors, include security requirements in contracts, and regularly audit third-party access and permissions.
- Strengthen Access Controls:
  - Implement multi-factor authentication (MFA) for all user accounts and use role-based access control (RBAC) to limit data access. Regularly audit and update access permissions.
- Enhance Security Monitoring:
  - Deploy intrusion detection and prevention systems (IDS/IPS), implement Security Information and Event Management (SIEM) solutions, and conduct regular vulnerability scans and penetration testing.

Script note : let start with one of the most common risks that is growing across every industry ‘Data breach’. This is when sensitive data gets exposed or stolen.

There are many causes behind data breaches, such as weak access controls, unpatched software, insider threats, or external attacks like advanced persistent threats (APTs) and hackers. These incidents can expose customer data, intellectual property, or even personal employee information, putting clients, the business and employees at significant risk.

Now, moving on to the impact. The consequences of a data breach are vast, but in terms of businesses, we can break them down into three big categories: reputation, competitiveness, and financial cost.

First, a company's reputation can be seriously ruined. And everyone knows that in industries like B2B SaaS, trust is everything. According to a 2023 study by IBM, a breach can cause 3-7% of customers to leave immediately, and new customers might take longer to sign up. Also negative media attention can last more than 1-2 years

For competitiveness, a 2023 report from McKinsey highlights that losing sensitive information could let your competitors catch up. And even worse if they get to hold your proprietary data, they can copy your unique features. This can result in losing your market share and delay your product development.

Finally, the financial costs can be huge. Consisting of investigating a breach, notifying affected people, facing lawsuits, having cybersecurity insurance level increase and dealing with regulatory fines that can go up to €20 million under GDPR, as specified by the European Commission.

So, what can businesses do to protect this

***Solutions** include using strong encryption to protect data, both when it's being sent and when it's stored. Make sure you also have good cyber insurance and update it regularly to cover new risks.*

You should also have a clear plan for handling a breach. Regularly test this plan, have a dedicated team ready, and prepare communication templates for different scenarios. And few more mentioned in slide

2, Cloud Service Provider Dependency risk

a. Explanation

***For those who don't know:**
They are companies that offer computing resources like servers, storage, and software over the internet. Businesses rent these services instead of managing their own infrastructure, benefiting from lower costs, better scalability, flexibility, enhanced security, and access to the latest technologies.

However, this dependency also introduces significant risk that organizations must beware.

Risk: Service outages beyond control

When technical issues occur with a cloud service, it becomes unavailable, impacting businesses that rely on it. For example, in 2020, a Google Cloud outage affected companies like Snapchat and Spotify, causing significant revenue loss and operational disruptions for those dependent solely on Google Cloud.

How are they impacted:

- Business Interruption:

  This interruption can lead to reduced productivity (especially for the employees who rely on cloud-based tools), missed opportunities, loss data and a failure to meet customer demands.

- Financial Losses:

  This risk leads to significant financial damage, including lost revenue from online transactions and sales. Besides, our business may also incur repair and recovery costs for IT assistance and data recovery tools.

- Customer Impact:

  When cloud services are disrupted, customers can experience significant frustration due to the inability to access services. This disruption can lead to diminished customer trust and satisfaction, as users are unable to engage with or use the applications and services they rely on.

Remediation:

Use multiple cloud providers: Split workloads across the two dominant providers so we are not overly dependent on one or the other, and to mitigate the impact of a platform-wide service disruption.

Negotiate clear Service Level Agreement: Ensure that performance expectations and penalties for downtime are clearly stated, that the provider is accountable and has compensation in place for outages.

3, Emerging Technology and Technical Risks

As we innovate with technologies like **AI**, **machine learning**, **IoT**, and **blockchain**, new vulnerabilities arise that need addressing. For instance, if someone manipulates the data AI relies on for inventory predictions, it could lead to costly overstocking or understocking. Similarly, IoT devices that track real-time inventory are vulnerable to attacks, potentially causing operational chaos. Even blockchain, though secure, can be exploited, threatening the integrity of our supply chain.

The challenge is that these technologies are relatively new, and security practices are still catching up, leaving us vulnerable to novel attack methods. This makes regular **vulnerability assessments**, adherence to **best practices**, and a **strong incident response plan** critical.

Beyond emerging technologies, there are also **technical risks** from rushing products to market, leading to **technical debt**. For example, Facebook's 2018 dating app faced technical issues due to a rushed launch, damaging their reputation. **Scalability** is another concern - Instagram struggled to handle its user growth in 2012, leading to outages until they moved to Amazon Web

Services.

To avoid these risks, we must plan for scalability early by using **cloud infrastructure** and **microservices**. Additionally, we can't ignore **cybersecurity threats** like ransomware—as seen in the 2021 Colonial Pipeline attack. Strong **cybersecurity measures** such as **multi-factor authentication**, **penetration testing**, and **employee training** are essential.

In short, the more we prepare for these technical risks now, the smoother things will run as we scale.

4, Geographic Risks:

a. **Explanation**

- **Caribbean (Data Center Location)**:
  - **Hurricanes/Tropical Storms**: The Caribbean is prone to hurricanes, which can lead to flooding, power outages, or destruction of infrastructure. For example, in 2017, Hurricane Maria devastated Puerto Rico, causing extended power outages that affected businesses for months. Cloud Providers like IBM and AWS have both taken significant steps to enhance disaster recovery and multi-region redundancy, especially in regions prone to natural disasters such as hurricanes. For instance, AWS has improved its *multi-region disaster recovery* by employing active-passive strategies across regions. This setup allows companies to quickly shift operations from a primary to a secondary region during a disaster, minimizing downtime. AWS uses tools like *Route 53*, *Lambda*, and *DynamoDB* to automate traffic failover between regions
    - SOURCES
      - Shah, Vaibhav, et al. “Implementing Multi-Region Disaster Recovery Using Event-Driven Architecture | AWS Architecture Blog.” *Aws.Amazon.Com*, 27 July

2021, aws.amazon.com/blogs/architecture/implementing-multi-region-disaster-recovery-using-event-driven-architecture/.

- https://cloud.ibm.com/docs/watsonxdata?topic=watsonxdata-hadr_wxd
- https://www.ibm.com/cloud/disaster-recovery

- **Impact:** Service disruptions due to power outages or infrastructure damage can lead to downtime, loss of customer trust, and potential revenue loss.
- **Mitigation**: The startup should implement **geo-redundancy**, using a hybrid cloud model to replicate critical infrastructure in a different geographic location (perhaps in Europe or North America). A cloud-based backup or distributed system can ensure minimal service disruption. Additionally, collaborating with local utility providers to secure priority power restoration contracts could mitigate downtime.

- **Remote Location**: The Caribbean is geographically far from both Eastern Europe and Paris, making it harder to mobilize resources quickly if there's an emergency. Consider the 2015 **Microsoft Azure outage**, where downtime was caused by hardware failure in its data center. Remote teams faced challenges in coordinating repairs due to the distance between the team and the site.
  - SOURCE: Nallainathan, Lavan. "Mitigating Downtime and Increasing Reliability: Strategies for Managing Complexity in the Cloud." *TECHCOMMUNITY.MICROSOFT.COM*, 30 May 2024, techcommunity.microsoft.com/t5/azure-architecture-blog/mitigating-downtime-and-increasing-reliability-strategies-for/ba-p/3810399.

        - **Impact:** Difficulty in quick physical access to the data center may result in prolonged downtime in the event of hardware failures or security breaches.
        - **Mitigation**: Establish remote management capabilities like **automated infrastructure orchestration** to minimize human intervention. Partnerships with local service providers for quick access to hardware repairs and physical security should be secured in case immediate intervention is needed. **Remote hands** services (local tech support hired by a third party) can bridge the gap when internal teams are far from the physical location.
- **Eastern Europe (Customer Base)**:
    - **Political/Economic Instability**: Economic or political shifts can affect the customer base significantly. Take the **2014 Ukrainian Crisis**, which caused financial instability and disrupted many businesses. Some tech companies, like **Luxoft**, had to shift focus to clients outside the region and diversify their customer base to mitigate the risk of economic downturns.
        - SOURCE: Makarin, Alexey. “Conflict and Intergroup Trade: Evidence from 2014 ...” *Alexeymakarin.Github.Io*, 2023, alexeymakarin.github.io/assets/Korovkin_Makarin_AER_2023.pdf.
        - **Impact:** Instability in Eastern Europe could result in customer churn, delayed payments, or reduced business from that region.
        - Expanding the customer base into more stable regions and offering flexible pricing models that adapt to local economic conditions will reduce the reliance on any one region. Regularly monitoring political and economic changes will allow the company to adjust its strategy proactively.

        - **Mitigation**: The company can **diversify its customer base** beyond Eastern Europe, expanding into other regions such as Western Europe or Southeast Asia. This diversification limits dependency on a single market. Additionally, flexible pricing models that adapt to the economic conditions of different regions could help maintain customer retention during economic crises.
    - **Regulatory Risks**: Data privacy laws in Europe, like the **GDPR**, may impose heavy penalties for data breaches. For example, in 2021, **Amazon** was fined €746 million by the EU for violating data privacy laws. If your company isn't fully compliant, it could face similar issues, especially if it's dealing with cross-border data transfers between Europe and the Caribbean.
        - **Impact:** Non-compliance with data privacy laws, especially GDPR, could lead to significant financial penalties and reputational damage.
        - **Mitigation**: Invest in strong **legal compliance frameworks** to align with both GDPR and local data regulations in the Caribbean. You may also consider **data localization** strategies to store sensitive data within the EU, minimizing cross-border legal issues. Regular legal audits should be conducted to stay ahead of shifting compliance needs.
        - **Remediation:** A comprehensive compliance strategy should be implemented, including hiring legal experts in both European and Caribbean jurisdictions to ensure full adherence to relevant regulations. Data localization strategies and ongoing audits will help ensure continued compliance and reduce the risk of violations. Implement strong encryption, security protocols, and ensure consent mechanisms are in place for all data transfers.

Script:

Our startup faces five key risks based on geography: hurricanes in the Caribbean, data center remoteness, political instability in Eastern Europe, GDPR non-compliance, and economic downturns. I'll cover how each impacts us and our strategies for mitigation.

First, hurricanes in the Caribbean are a high-priority risk due to the potential for power outages and infrastructure damage. To mitigate this, we'll use geo-redundancy by replicating our infrastructure in Europe or North America. This ensures seamless service during storms. Partnering with local utilities for priority power restoration will also minimize downtime.

Next, the remoteness of our data center presents a challenge. Delayed responses to hardware failures or security breaches could lead to extended downtime. Strengthening remote management tools and working with local providers will enable faster recovery without on-site intervention, reducing this risk.

Political instability in Eastern Europe, like the 2014 Ukrainian crisis, could disrupt our customer base. We'll mitigate this by diversifying into more stable markets, such as Western Europe and Southeast Asia, and offering flexible pricing to retain customers during crises.

Non-compliance with GDPR is another high-priority risk, given the potential for hefty fines and reputational damage. We'll ensure compliance through data localization, regular audits, and robust encryption, reducing our legal risks.

Lastly, economic downturns could impact customer payments, especially in Eastern Europe. While this is a lower-priority risk, we'll mitigate it by diversifying our customer base and offering flexible payment plans during tough times.

Each of these risks impacts different aspects of our business. Hurricanes and remoteness affect our infrastructure, while political instability and economic downturns impact revenue. GDPR violations could damage our reputation and lead to fines. Geo-redundancy, remote management, customer diversification, and compliance measures will reduce these risks. Hurricanes and remote access issues are more likely, while political instability and GDPR risks, though less frequent, could have severe consequences.

If these risks materialize, our Disaster Recovery Plan will focus on restoring services quickly. For hurricanes, we'll switch to backup locations within hours. Remote access issues will be resolved within 12 to 24 hours. Political instability may take longer to address, but diversification will protect revenue. GDPR breaches will require immediate legal response and audits. Communication with internal teams, customers, and stakeholders will be key during any incident, using tools like remote infrastructure management and legal compliance systems.

Our Business Continuity Plan ensures degraded but functional service during incidents. Geo-redundant infrastructure and automated systems will maintain operations during hurricanes or technical failures. For political instability or economic downturns, our diversified customer base will sustain revenue. GDPR-related incidents may require pausing data services, but other operations will continue. Once the disaster is resolved, we'll quickly switch back to full service and inform customers that operations are normal.

5, Customer Service Risks:

a. **Explanation:**
   i. Time zone differences between Paris and Eastern Europe could lead to delays in customer support, similar to the issue Slack faced in 2019, which prompted them to introduce 24/7 support. This lag can negatively impact customer satisfaction and brand reputation.

b. Impact:
   I. **Brand Reputation:** Negative reviews on platforms like G2 or Capterra can deter potential customers. Poor support in B2B SaaS can lead to a 20-30% decrease in referral business.
   II. **Operational Efficiency:** Inefficient support processes may increase the cost per ticket by 30-50% and divert resources, delaying feature releases by 10-20%.
   III. **Revenue Impact:** Poor customer service can result in a 20% loss in repeat business and a 25-35% decrease in upsell and cross-sell opportunities due to diminished customer trust.

c. Remediation:

i. **Customer Feedback Loop:** Regularly collect and analyze customer feedback to improve support processes and identify training needs.
ii. **24/7 Support Coverage:** Set up a round-the-clock customer service team by hiring agents across multiple time zones and use a follow-the-sun model for continuous coverage.
iii. **AI-Powered Support:** Deploy AI chatbots for simple queries to reduce response times and use machine learning to direct complex issues to appropriate human agents.

Now let see about Customer service risk which is caused by the different time zone. It could lead to delays in customer support. This lag can negatively impact customer satisfaction and brand reputation.

Speaking of impact I slightly mention the brand image already. For example the negative review on platforms like G2 or Capterra can deter potential future customers. In the B2B SaaS sector, poor customer support can lead to a 20-30% drop in referral business.

*So, what can be done?***,** *We found a few remediation strategies for this:*

1. *Implement a Customer Feedback Loop to regularly gather and analyze feedback to improve support processes.*
2. *Set up 24/7 Support Coverage by hiring agents across multiple time zones.*
3. *Use AI-powered Support for simple questions to reduce response times, while more complex issues are directed to human agents.*

Continuity Plan

- Maintaining degraded service:

It's important to ensure access to essential services critical for customer operations, even if some features remain limited. For example, basic data access could still be available while more advanced analytics features are temporarily disabled.

Our focus will be on prioritizing core functionalities like basic inventory management. To achieve this, we'll leverage our multi-cloud strategy, shifting workloads to alternative cloud providers as needed.

- Services might be sacrificed:

Advanced functionalities that are not essential for immediate operations, such as detailed reporting tools or optional integrations. Less-essential services (only in the period of disaster): advanced analytics, experimental features, and region-specific functions

- Impact to customer:

During an incident, customers may encounter restricted access to certain features, slower response times. Some functionalities will be temporarily unavailable, limiting the use of essential tools. This, in turn, might impact overall productivity and customer satisfaction. However, these disruptions are among the mildest impacts as core services will continue to operate, reducing the overall effect on business continuity.

- Switch back to full service after resolving the disasters:

Once the issue is resolved, services will be restored progressively, starting with careful testing and verification to ensure that all systems are operating securely as expected. We will reroute traffic as necessary, reintroducing features step by step to minimize disruption.

After full services have been restored, we will conduct a comprehensive review. This analysis will focus on evaluating the incident response, identifying potential areas for improvement, and making updates to the business continuity plan accordingly.

Conclusion

In conclusion, our startup faces several key risks, including geographic challenges, customer service issues, and the risks associated with emerging technologies. However, by implementing proactive risk management strategies such as geo-redundancy, scalable infrastructure, and strong cybersecurity measures, we can reduce these threats and ensure business continuity. Prioritizing customer satisfaction through 24/7 support, AI-driven solutions, and ongoing feedback will strengthen our brand and retain customer trust. Finally, maintaining GDPR compliance and preparing for future growth will position us for sustainable success in the competitive SaaS market..

That's for today. I hope you enjoy our presentation.

We are pineapple inc. and this is a risk analysis from us, thank you and have a great day.

References:

1. https://thrivedx.com/resources/article/4-damaging-data-breach-effects
2. https://assets.kpmg.com/content/dam/kpmg/ca/pdf/2018/03/cloud-computing-risks-canada.pdf
3. https://www.ibm.com/reports/data-breach
4. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
5. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en
6. https://rsmus.com/insights/services/risk-fraud-cybersecurity/the-cost-of-a-data-breach.html

7. https://www.hcltech.com/trends-and-insights/understanding-cloud-outages-causes-consequences-and-mitigation-strategies
8.