Category 1

The Cybercare Defender

HEALTHCARE CYBERSECURITY STRATEGY

Protecting healthcare systems and patient data with simple, practical, and trusted solutions

+15555555555

www.cybercaredefender.ca

Kootenai Health Ransomware Attack

Cybersecurity threats in healthcare are growing, as seen in the recent ransomware attack on Kootenai Health. Healthcare organizations store valuable data, making them prime targets for cybercriminals. A breach can lead to financial losses, delays in patient care, and even risk lives.
Kootenai Health's attack highlights key vulnerabilities, including lack of employee training, outdated systems, and poor response strategies. This hackathon will explore these issues, examine the weaknesses revealed, and come up with practical solutions to better protect the healthcare sector from future threats.

Problem Statement

1

Lack of Employee Cybersecurity Awareness

A major issue is the lack of basic security protocol awareness among employees. Research shows that 43% of employees admit to clicking on phishing emails (Proofpoint, 2023), which makes organizations vulnerable to cyberattacks. In fact, 72% of healthcare organizations report being victims of phishing attacks (HIMSS, 2023), illustrating the scale of the threat. These breaches can easily lead to malware downloads, which then trigger ransomware attacks, as seen with Kootenai Health.

2

Insufficient Security Training Programs

Many healthcare organizations, including Kootenai Health, suffer from insufficient security training for their staff. This can have devastating effects, as evidenced by the extended downtime Kootenai Health experienced during the ransomware attack, lasting several weeks. According to Varonis (2023), the average cost of downtime in healthcare organizations is estimated at $7,900 per minute. This downtime not only affects the financial standing of the organization but directly impacts patient care, delaying access to critical health data, prescriptions, and treatment, ultimately jeopardizing patient safety.

3

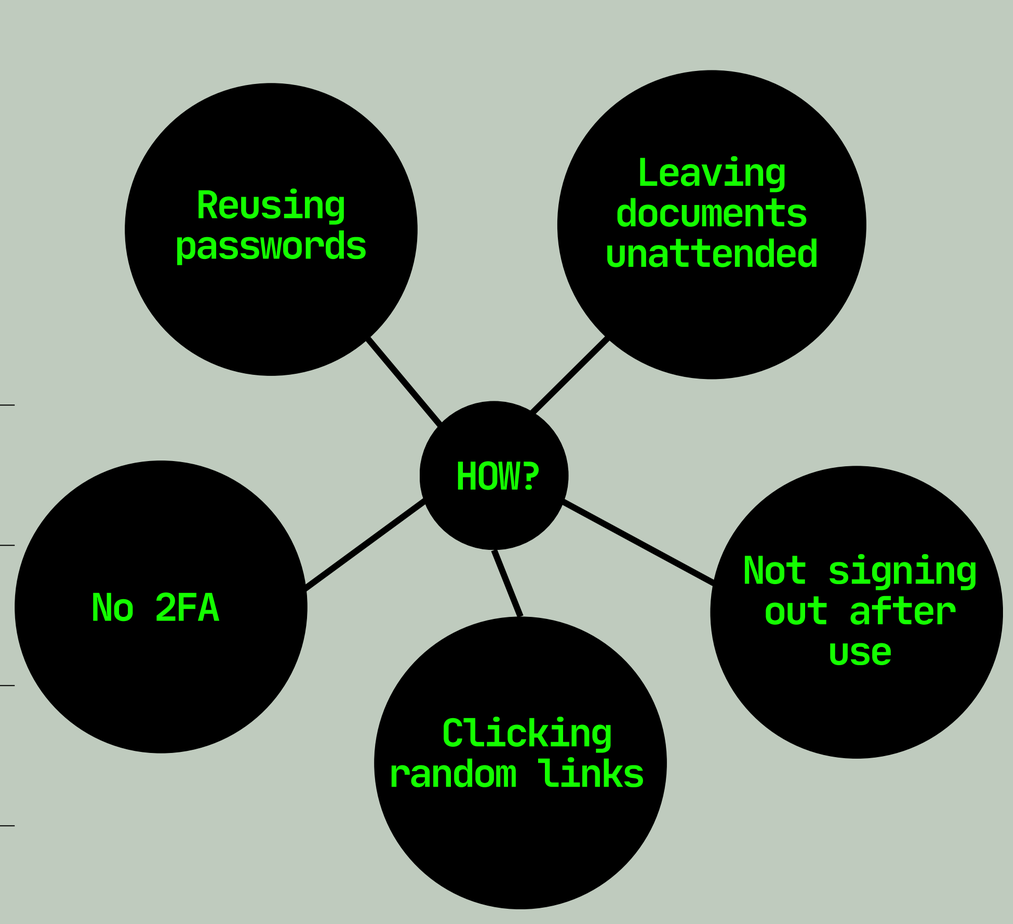
Outdated Threat Detection Systems:

Kootenai Health’s outdated infrastructure was another major vulnerability. The organization’s security systems were unable to detect the sophisticated attack in time, allowing the ransomware to spread and disrupt their operations. Advanced intrusion detection systems (IDS) and next-generation firewalls are essential to prevent such attacks. Without these, organizations like Kootenai Health remain at risk of falling victim to evolving threats, as cybercriminals continuously improve their tactics.

How can security risks occur?

Cybersecurity starts within the culture. A poor emphasis on proper protocols could lead to potential damage overtime. This can happen because:

Reusing passwords	**Using the same password across multiple accounts makes it easier for attackers to gain unauthorized access if one account is compromised.**
Leaving documents unattended	**Sensitive information left exposed, whether physically or digitally, can be exploited by unauthorized individuals.**
Not signing out after use	**Failing to log out from sensitive accounts leaves information vulnerable to unauthorized access.**
Clicking random links	**Falling for phishing scams or malware-laden links can compromise systems and lead to data breaches.**
No 2FA	**Relying solely on passwords without an additional layer of verification makes accounts more susceptible to hacking.**



HoloLens-Integrated Red Team Exercises
Use Microsoft HoloLens for immersive, real-world cybersecurity testing (Red Team and Blue Team), incorporating AR to visualize vulnerabilities and risks.

Cybersecurity Credit Score System
Implement a system to evaluate and score employee cybersecurity practices, offering feedback and opportunities for improvement.

Cybersecurity Awareness Campaign
Focus on raising awareness about cybersecurity risks and best practices through workshops, training, and engagement programs.

AR-Enhanced Security Training
Develop and deploy augmented reality (AR)-based training simulations to improve employee understanding of security protocols in real-time scenarios.

Enhance Security Culture Across the Organization
Foster a proactive cybersecurity culture where employees are equipped with the knowledge and tools to identify, mitigate, and prevent cyber threats.

To Safeguard Patient and Employee Data
Protect sensitive information by implementing cutting-edge cybersecurity practices that ensure the privacy, integrity, and availability of healthcare data.

Trust, Responsibility, Continuous Improvement
Uphold a strong commitment to data security through transparency, ethical behavior, and constant innovation to adapt to evolving threats.

PROJECTS **INITIATIVES** **OBJECTIVES** **MISSION** **VISION**

SOLUTION

Red Team

- Tasked with going into the organization, while utilizing hidden cameras will go through and try and test out various vulnerabilities such as:
  - Gathering intel on potential pressure points in the organization
    - Unsecured points / devices.
    - Poorly Guarded positions or unlocked areas / terminals.
  - Physical / Digital Penetration Testing
    - Attempting to gain access to restricted areas and devices.
    - Attempt access to unsecured protocols, vulnerable software, and direct phishing.

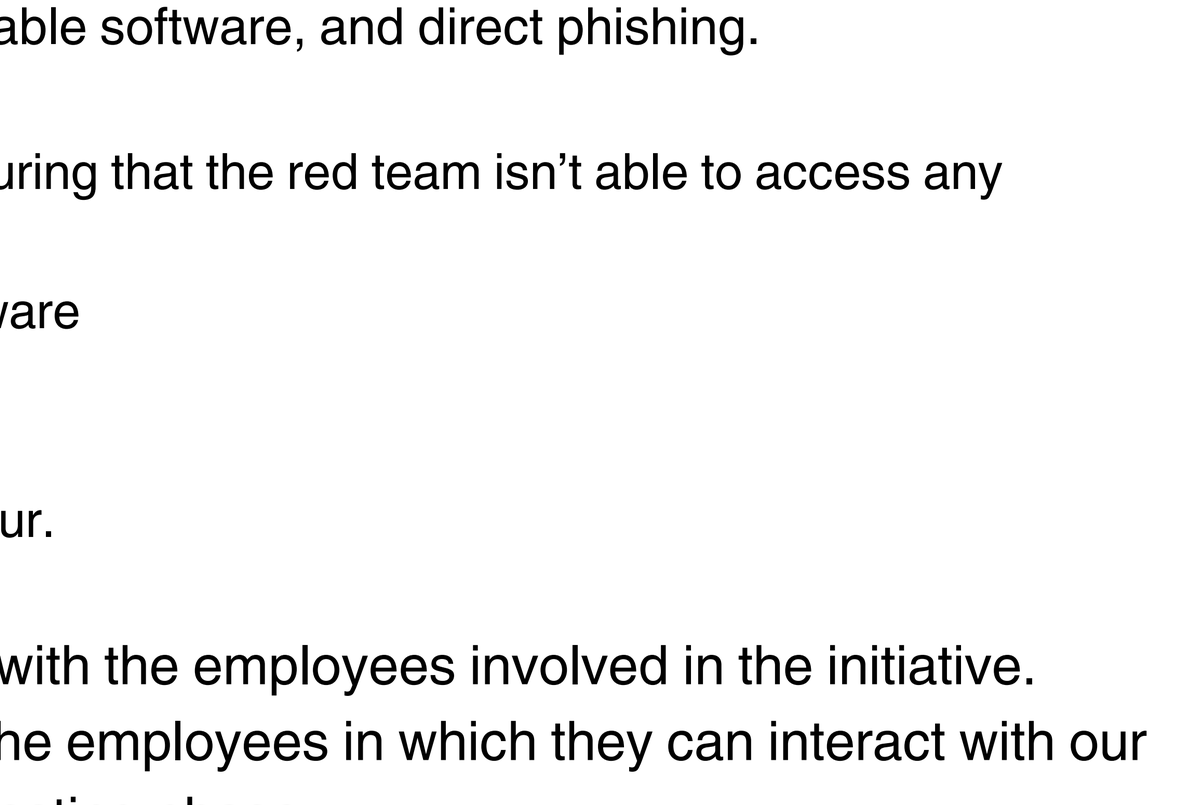
Blue Team

- Tasked with monitoring various digital aspects, and ensuring that the red team isn't able to access any network vulnerabilities.
- Additionally this team will mainly target our training software
  - Overseeing the various breeches.
  - Monitoring the red teams activity.
    - Tracking and flagging potential risks as they occur.

Purple Team

- A combination of the blue and red teams, mixed in with the employees involved in the initiative.
  - This will involve an opt-in testing process with the employees in which they can interact with our AR glasses as will be further mentioned in the testing phase.

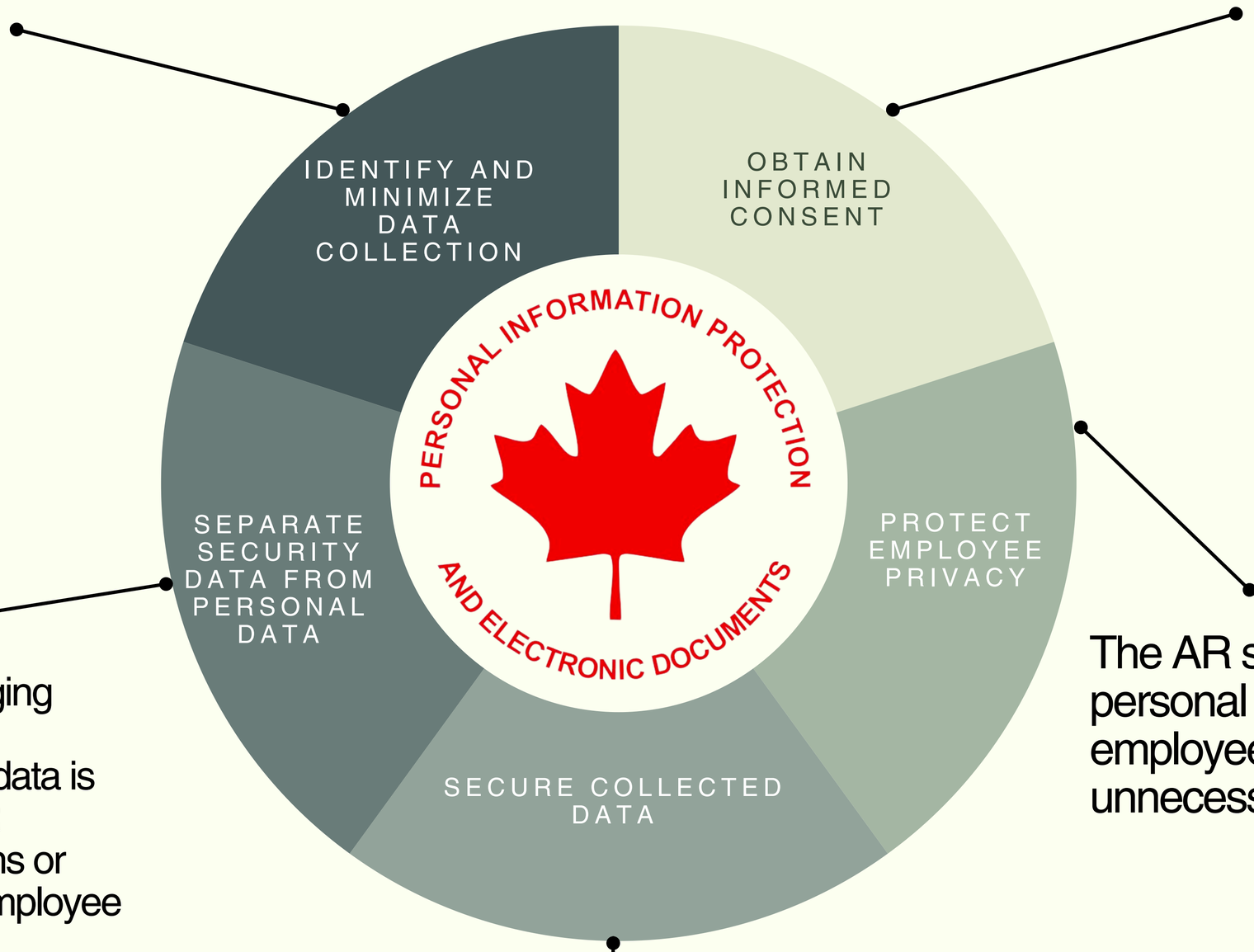
- The Cybersecurity Credit Score starts at 1000, with points added for addressing AR-flagged vulnerabilities, like securing devices and deducted for missed risks, such as ignoring alerts. AR enhances this system by highlighting danger zones in real-time, showing how employee actions impact the score. Bonus points are awarded for minimal breaches, encouraging proactive security practices.
- At the end of the simulation, employees review incidents through AR, seeing how their actions influenced the final score. This gamified approach engages teams, reinforces cybersecurity habits, and motivates continuous improvement.



Compliance with PIPEDA

Our AR system will collect only the data required to identify and address security vulnerabilities.
Whenever possible, all data will be collected onsite and within the appropriate region to ensure compliance with privacy regulations.

Employees will be fully informed of the program's purpose after the red and blue team exercises are complete.
Participation is optional, and employees who choose not to take part will be granted opt-out provisions in the program.



Use it solely for flagging behaviors.
Ensure that the AR data is not linked to any HR performance systems or other databases / employee records.

The AR system will obscure personal data to safeguard employee privacy and prevent unnecessary exposure.

Encrypt all data received.
Allow access only to authorized personnel.
Retention limits will be strictly enforced to ensure data is stored only for as long as necessary.

How can we communicate this?

At the end of each security screening, data is thoroughly analyzed, highlighting areas where security risks were introduced and marking the locations where these incidents occurred. Employees are then provided with AR glasses that offer an in-depth view of the risks they could have prevented, along with visual cues to enhance their understanding. Additionally, vulnerabilities caused by other employees are displayed, allowing team members to learn from one another's mistakes, improve collectively, and maintain anonymity. After the screening, the organization receives a Cybersecurity Credit Score, reflecting its overall performance, with actionable insights on areas to improve for the next round. This continuous feedback loop fosters a culture of learning and improvement, empowering employees to take a proactive role in maintaining security.

Technological Infrastructure

Hardware

Microsoft Hololens 2 - Industrial Edition

CAD $6,389.00

Tested and standardized (ISO 14644-1 Class 5 rating) with regulations that support clean rooms and hazardous locations.

Alternative products (such as Meta’s Orion) could be used if the right permissions are obtained.

Software

Using Microsoft Mixed Reality Toolkit

- Uses the unity engine and supports prototyping through their in-editor simulation which allows us to see the changes immediately.
- Can be used for observing the data received by the red team, to customize the received information and display which points were hazards, or direct incidents that could have serious security risks.
    -

HoloLens Spatial Awareness

- The HoloLens utilizes a built-in system that employs mesh mapping to create a virtual representation of the room, which is then displayed through the AR glasses.
    - Note: This requires the red team to observe the facility with the glasses specifically.

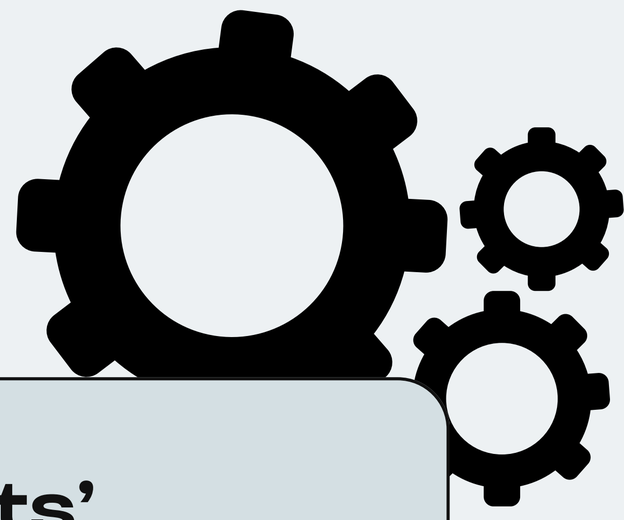
TensorFlow Object Detection API

- Observe the facility and train a custom model on the unique objects and label them (medical device, etc.).
- These will be bounding boxes set up (Red for serious risks and yellow for danger).
- They can instead analyze footage from those parts, cutting viewing time.

Cost Considerations and Resources

- AR glasses are becoming more affordable and advanced over time, making them increasingly feasible for large-scale deployment.
- There are ample resources available for integrating location tagging in AR applications, which will streamline development efforts.

Impact



Protect Millions of Patients' Information

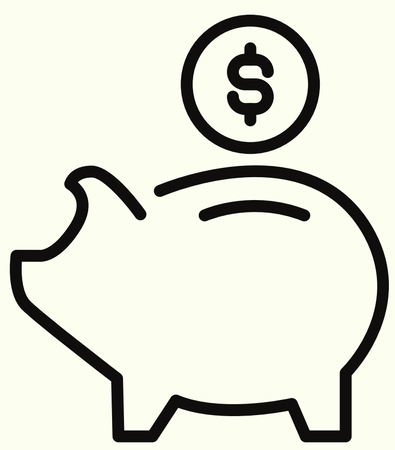
Safeguard sensitive personal and medical data from unauthorized access and breaches, ensuring trust and compliance with privacy standards.

Reduce Risk of Fraud and Cyber Threats.

Mitigate the risk of phishing, ransomware, and other cyber threats that target both the organization and its patients.

Support Employee's Privacy

Implement robust measures to secure employee data, ensuring their personal information remains confidential and protected.



Saves money

Avoid the high costs associated with data breaches, including legal penalties, reputational damage, and operational downtime, by investing in proactive cybersecurity measures.

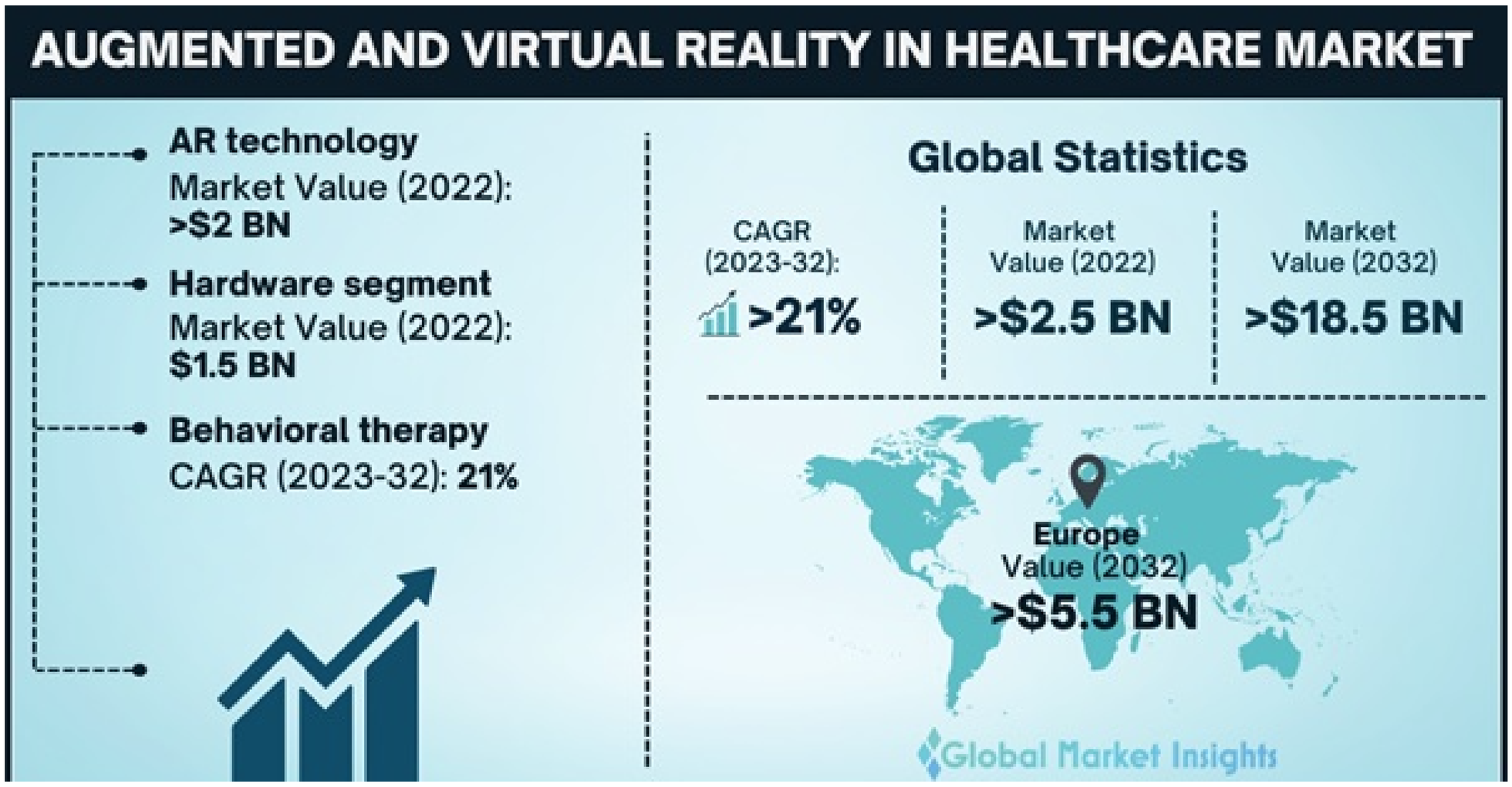
Maintain Operational Continuity

Prevent disruptions caused by cyberattacks, such as ransomware, which can halt critical healthcare services.

Enhance Patient Trust

Demonstrate commitment to protecting patient data, fostering loyalty and confidence in the organization's services.

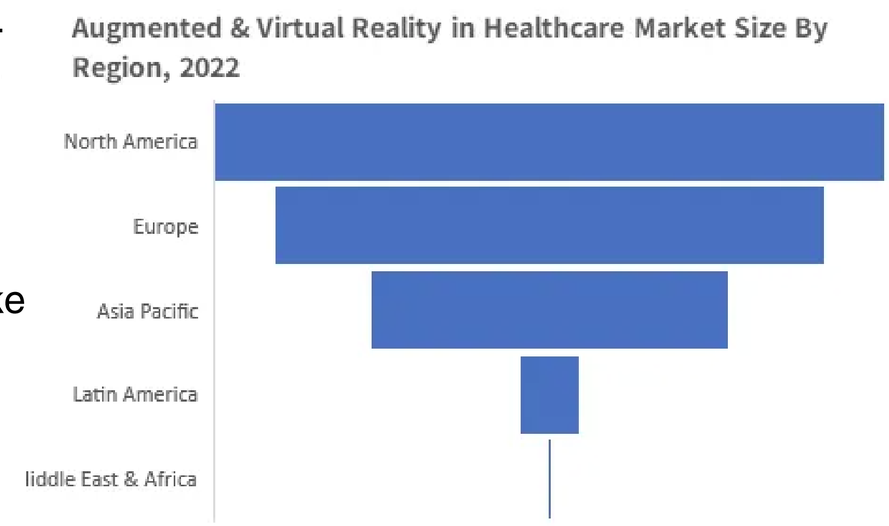
Opportunity and market size



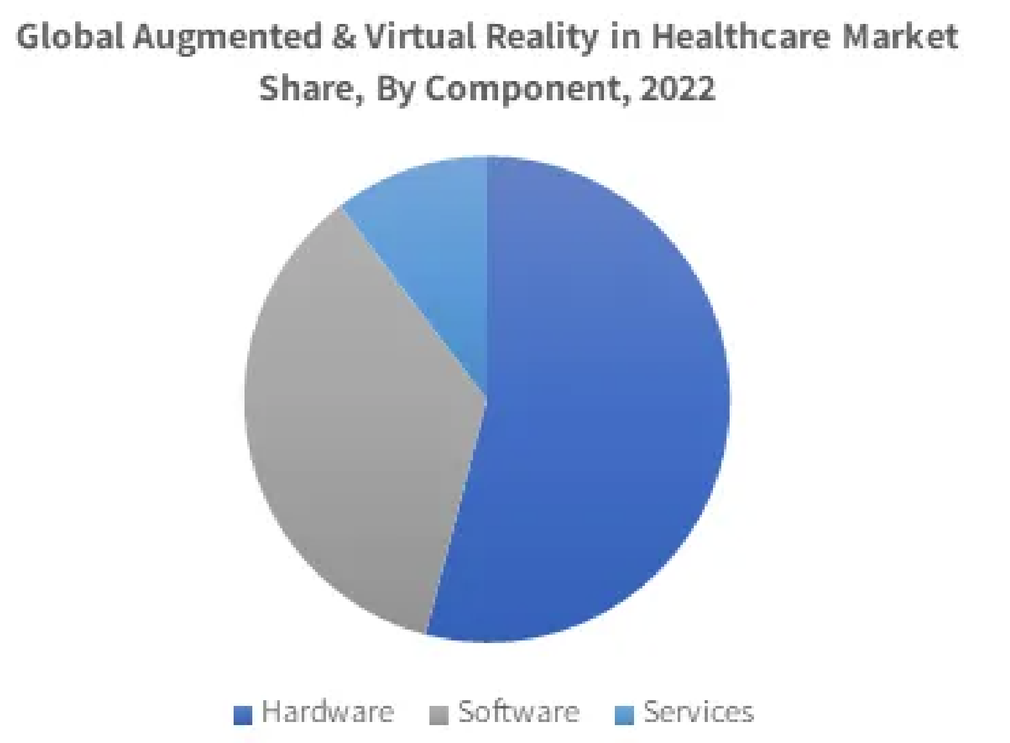
North America’s Lead

- The AR/VR healthcare market in North America is expected to experience remarkable growth, with a forecasted compound annual growth rate (CAGR) of 30-35% from 2024 to 2029 . This is driven by a surge in both public and private sector investments in research and development, as well as an increasing adoption of these technologies in healthcare settings, including hospitals, clinics, and surgical centers. With North America leading in terms of technological infrastructure and innovation, this creates an ideal market for introducing specialized AR solutions, like those focused on enhancing cybersecurity awareness in healthcare environments.

- As cybersecurity concerns continue to grow in healthcare, integrating AR/VR technology to improve security practices offers a timely and unique opportunity. These technologies are not only being utilized for improving patient care and training but are now extending to cybersecurity education and risk management. The combination of high demand for AR/VR solutions and the critical need for robust cybersecurity creates a promising avenue for your cybersecurity-focused AR glasses solution.



Source: www.gminsights.com



Source: www.gminsights.com

- Healthcare organizations are under increasing pressure to safeguard sensitive data as cyberattacks on the sector continue to rise. With valuable patient information being a prime target, healthcare systems face growing risks from ransomware, data breaches, and compliance violations. Traditional cybersecurity training often falls short in preparing staff for the real-world tactics hackers use.

- Integrating AR technology into cybersecurity training can be a game changer for healthcare institutions. By immersing employees in interactive, scenario-based simulations, AR helps them recognize vulnerabilities and respond to threats instantly. For example, using AR glasses, staff can be alerted in real-time about potential security breaches, such as unauthorized access or phishing attempts. This hands-on training improves awareness and helps staff quickly detect and mitigate risks, reducing the chance of costly human errors.

- This fusion of AR with cybersecurity training can lead to stronger defense mechanisms, ensuring that healthcare organizations are better equipped to protect sensitive data and keep systems running smoothly. By empowering employees with the knowledge and tools to identify threats as they arise, healthcare institutions can significantly improve their overall security posture.

Estimated Cost Table

Cost/terms	Short term	Medium-term	Long-term
AR Implementation	$6,000-$10,000 (1, 2 devices)	$12,000–$20,000 (maintenance, scaling to 4 devices)	$24,000–$30,000 (scaling to 6–8 devices)
Cybersecurity tools	$5,000–$8,000(program creation, initial rollout)	$4,000–$6,000 (updates, targeted refreshers)	$6,000–$10,000 (continuous updates, new modules)
Audits (Red Teaming)	$5,000–$8,000 (1–2 sessions, pilot testing)	$7,000–$10,000 (5–10 sessions, advanced threats)	$10,000–$15,000(frequent sessions, automation integration)
Marketing related costs	$3,000–$5,000 (basic marketing)	$5,000–$7,000(expanded awareness campaigns)	7,000–$10,000 (scaling up marketing)
OTHER COSTS	$2,000–$3,000 (incidental costs)	3,000–$4,000(hardware upgrades, add-ons)	$6,000–$8,000 (new infrastructure setup)
TOTAL COST	$30,000–$48,000	$42,000–$57,000	$62,000–$92,000

Break-even point

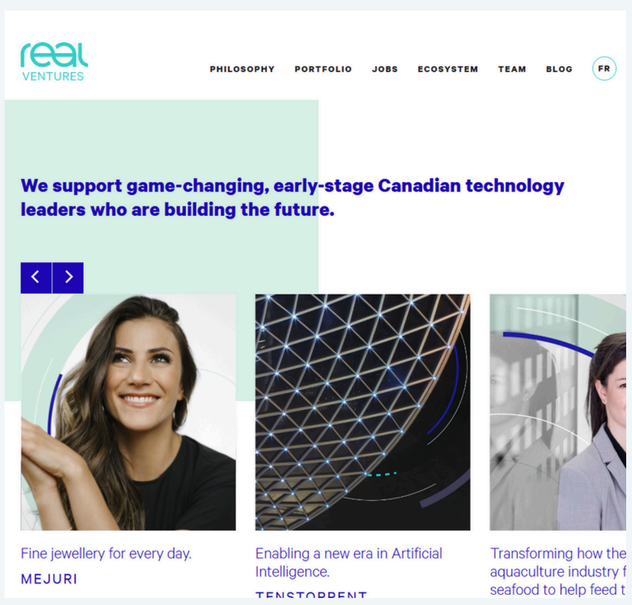
$87,000 in revenue

Break-even is surpassed comfortably, with profits growing between $54,000–$78,000

Revenue-Profit Table

PHASES	Revenue (CAD)	Costs (CAD)	Profit (CAD)	Profit Margin (%)
Short-Term	$30,000–$50,000	$27,000–$48,000	$0–$3,000	0–6%
Medium-Term	$70,000–$100,000	$38,000–$57,000	$33,000–$43,000	33–43%
Long-Term	$110,000–$150,000	$62,000–$92,000	$48,000–$58,000	40–45%
Overall	$210,000–$300,000	$156,000–$222,000	$54,000–$78,000	26–30%

Funding, investment, grants and partnership



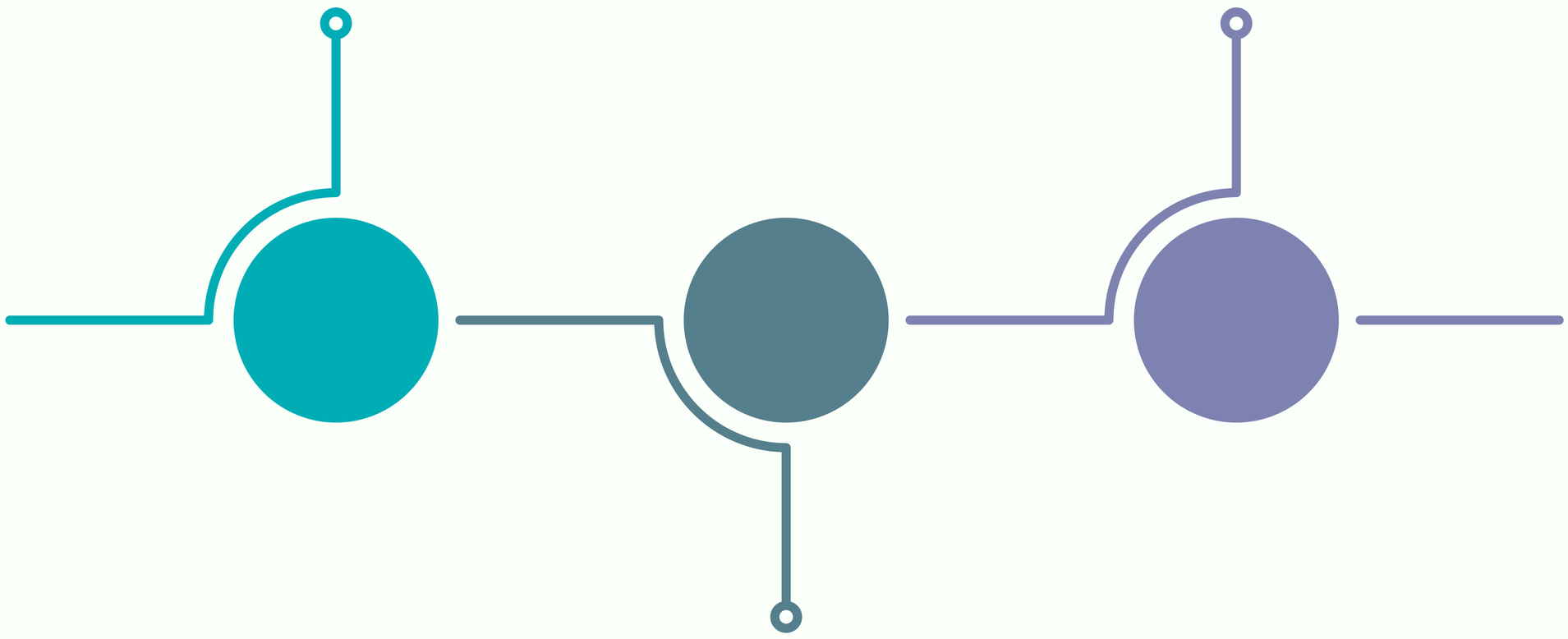
Detailed Implementation

Objective: Raise immediate awareness, establish security measures, and assess vulnerabilities.

1. Employee Behavior and Awareness Training
   - Mandatory Training: 2-hour workshops and e-learning modules covering risks (password reuse, phishing) and best practices (2FA, securing devices).
   - Example: Highlight how employee actions led to the 2024 Kootenai Health ransomware attack.
   - Awareness Campaigns: Weekly email tips, posters near workstations, and a "Cybersecurity Champions" program for department contacts.
2. Strengthen Technical Security Measures
   - Tools: Deploy Bitwarden for password management, use Cloudflare for DNS protection and DDoS mitigation, enforce HTTPS on internal systems.
   - Device Policies: Mandate full-disk encryption (e.g., BitLocker) and automatic screen lock after 2 minutes.
3. Red Team Testing
   - Simulations: Run phishing campaigns and assess responses, conduct physical tests (e.g., bait USB drives), and evaluate weaknesses in login procedures (e.g., unattended desktops).

Objective: Establish sustainable systems and continuously enhance cybersecurity awareness.

1. Purple Team Integration with AI
   - Merge Red and Blue team insights into a Purple Team for proactive monitoring.
   - Use AI tools (e.g., TensorFlow) for automated risk detection.
2. AR Glasses Expansion
   - Scale AR glasses deployment for real-time security feedback.
   - Use TensorFlow to identify risks in physical and operational environments.
3. Advanced Employee Education
   - Partner with AR hardware developers (e.g., Microsoft, Meta) for updated training.
   - Host annual cybersecurity summits to share trends and performance.
4. Continuous Security Testing
   - Run monthly phishing campaigns and quarterly system audits for regulatory compliance.
5. Policy Development
   - Establish a Cybersecurity Governance Committee for ongoing protocol updates.
   - Ensure PIPEDA compliance through regular data retention and privacy policy reviews.



1. Advanced Red/Blue Team Exercises
   - Red Team Activities:
     - Advanced phishing (e.g., targeted spear phishing via Teams or SharePoint spoofing).
     - Simulate insider threats (e.g., employee impersonation using fake credentials).
   - Blue Team Defense:
     - Train IT staff to recognize and counter advanced threats in real-time.
     - Use tools like Snort for intrusion detection and advanced log monitoring.
2. Deployment of AR Glasses for Feedback
   - Procure Microsoft HoloLens 2 units ($6,389/unit).
     - 5 units for training teams = ~$32,000.
   - Develop a custom application using Microsoft Mixed Reality Toolkit to:
     - Overlay flagged vulnerabilities (e.g., unattended devices, unsecured documents).
     - Provide real-time feedback after exercises (e.g., red for high risks, yellow for moderate risks).
   - Train employees with AR scenarios simulating:
     - Malware exposure when clicking suspicious links.
     - Data loss from unattended devices.
3. Gamified Cybersecurity Credit System
   - Create a dashboard that tracks:
     - Departmental performance in red/blue team exercises.
     - Individual scores for avoiding phishing attempts or flagging potential breaches.
   - Use metrics to gamify improvement with rewards like "Top Cybersecure Team of the Month."
4. System Upgrades
   - Address outdated systems: Update all software, including SharePoint and Teams.
   - Secure critical data (e.g., health records, SINs) with enhanced encryption protocols.