Business Profile

Ryan Coon

CYB-690

Dr. Kimberly Ford

September 3, 2025

**Business Name**

RC Cybersecurity

**Mission Statement**

At RC Cybersecurity, our mission is to protect the digital landscape of businesses and individuals by providing comprehensive and innovative cybersecurity solutions. We are committed to proactive defense, utilizing state-of-the-art technology to anticipate, detect, and neutralize threats before they can cause harm. Our approach emphasizes empowerment through knowledge, as we believe that educating our clients is crucial in fostering a culture of cybersecurity awareness. By offering tailored solutions that align with each client’s unique needs, we ensure that they are equipped to tackle their specific challenges. Integrity and trust are at the core of our operations, guiding our relationships with clients through transparency and ethical practices.

**Vision Statement**

To be the most trusted and innovative cybersecurity partner, creating a secure digital future where businesses can thrive without fear of cyber threats.

**Goals and Objectives**

* Enhance Client Security Posture - Reduce client-reported security incidents by 30% within the first year of engagement.
* Expand Market Reach - Establish partnerships with 15 new enterprise-level clients within two years.
* Innovate New Service Offerings – Launch two new proprietary cybersecurity tools within 18 months.
* Cultivate Expertise – Achieve 95% client satisfaction rating for technical support and consultation.
* Foster Talent – Maintain a 90% employee retention rate through continuous professional development and a supportive work environment.

**Industry Information/Experience**

The cybersecurity industry is characterized by rapid technological advancements, a persistent and evolving threat landscape, and a growing demand for skilled professionals. RC Cybersecurity leverages extensive experience in threat intelligence, incident response, vulnerability management, and security architecture design across various sectors, including finance, healthcare, and e-commerce.

**Major Stakeholders**

* Clients – Businesses of all sizes seeking robust cybersecurity solutions.
* Employees – Highly skilled cybersecurity professionals and support staff.
* Investors/Shareholders – Providing capital and strategic guidance.
* Technology Partners – Collaborating on innovative security tools and platforms.
* Regulatory Bodies – Ensuring compliance with industry standards and data protection laws.

**Business Organizational Chart**

A black and white diagram with words

Description automatically generated with medium confidence

**Products and Services**

**Main Products/Service Offerings**

* Managed Security Services (MSS) – 24/7 monitoring, threat detection, and response.
* Vulnerability Assessment & Penetration Testing – Identifying and mitigating system weaknesses.
* Incident Response & Forensics – Rapid containment, eradication, and recovery from cyber incidents.
* Cloud Security Solutions – Securing cloud infrastructure and data.
* Cybersecurity Consulting – Strategic guidance, policy development, and compliance assistance.
* Security Awareness Training – Educating employees to prevent human-factor breaches.
* Threat Intelligence Platform – Proactive identification of emerging threats.

**Consumer Base**

* Small and Medium-sized Enterprises (SMEs) – Providing accessible and scalable security solutions.
* Large Corporations – Offering advanced, tailored security frameworks and managed services.
* Government Agencies – Ensuring the protection of sensitive public data.
* Financial Institutions – Meeting stringent regulatory requirements and protecting financial assets.
* Healthcare Providers – Safeguarding electronic patient data (ePHI) and critical infrastructure.

**Technology and Security Solutions**

Based on our goals to enhance client security posture, expand market reach, innovate service offerings, and foster talent, RC Cybersecurity deploys a robust suite of technology and security solutions:

**To Enhance Client Security Posture & Foster Resilience:**

* Managed Detection and Response (MDR) Platform - We utilize a 24/7 Security Operations Center (SOC) integrated with Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools. This allows us to monitor client environments, detect threats in real-time, and initiate rapid response.
* Advanced Threat Intelligence Feeds - We integrate multiple threat intelligence sources to proactively identify emerging threats, vulnerabilities, and attack vectors relevant to our clients' industries.
* Vulnerability Management Tools - Regular scanning and assessment of client systems and networks are performed to identify and prioritize vulnerabilities for remediation.
* Security Orchestration, Automation, and Response (SOAR) Platform - This enables us to automate repetitive security tasks, streamline incident response workflows, and reduce manual intervention, boosting efficiency and response times.
* Next-Generation Firewalls (NGFW) and Intrusion Prevention Systems (IPS) - These are deployed to enforce network security policies, inspect traffic, and block malicious activities at the network perimeter.

**To Expand Market Reach & Cultivate Expertise:**

* Secure Cloud Infrastructure - We leverage robust cloud security solutions like AWS Security Hub, Azure Security Center, to host our services and client data, ensuring scalability, availability, and compliance.
* Customer Relationship Management (CRM) System - A secure and efficient CRM is used to manage client interactions, track sales pipelines, and support client success initiatives.
* Knowledge Management System - A centralized repository for best practices, threat research, case studies, and training materials ensures continuous learning and expertise development across our team.
* Secure Collaboration Tools - Encrypted communication and collaboration platforms are used for internal teams and secure client communication.

**To Innovate Service Offerings:**

* Research and Development (R&D) Lab - We maintain a dedicated environment with access to cutting-edge security technologies, sandboxing capabilities, and development tools for creating proprietary solutions.
* AI and Machine Learning Platforms - We leverage AI/ML for advanced threat detection, behavioral analysis, and predictive security modeling.
* Secure Development Lifecycle (SDL) - We implement secure coding practices and regular security testing for all internally developed software and tools.

**To Foster Talent:**

* Secure HR and Payroll Systems - Sensitive employee data is protected with robust access controls and encryption.
* Learning Management System (LMS) - This is used for delivering and tracking cybersecurity training and professional development programs for employees.
* Secure Remote Access Solutions - VPNs and multi-factor authentication (MFA) are provided for employees working remotely, ensuring secure access to company resources.

**Overall Security Posture for RC Cybersecurity -** For our own operations, we implement foundational security measures including:

* Multi-Factor Authentication (MFA) - For all internal access to systems and data.
* Data Encryption - At rest and in transit for all sensitive company and client data.
* Regular Security Audits and Compliance Checks - To ensure adherence to internal policies and external regulations.
* Employee Security Awareness Training - Regular training for all employees on phishing, social engineering, and secure data handling practices.
* Business Continuity and Disaster Recovery (BC/DR) Plans - To ensure operational resilience in the event of a disruptive incident.

**Business Continuity Plan (BCP) and Disaster Recovery (DR)**

**Business Continuity Plan**

Our Computer Security Incident Response Team (CSIRT) is a multi-disciplinary unit comprising experts from various departments, ensuring a holistic response capability. Key roles within the CSIRT include:

* Incident Response Manager - Oversees the entire IR process, coordinating team efforts and stakeholder communication.
* Security Analysts - Conduct initial triage, investigation, and containment of security incidents.
* Forensic Specialists - Perform in-depth analysis of compromised systems to determine the scope and cause of an incident.
* IT Infrastructure Specialists - Provide technical expertise on affected systems and networks for recovery.
* Legal Counsel - Advises on legal and regulatory implications during and after an incident.
* Communications Lead - Manages internal and external communications related to the incident.
* Human Resources Representative - Addresses personnel-related issues arising from an incident.

**Incident Preparation and Planning**

Our preparation phase is continuous and iterative:

* Incident Response Plan (IRP) - A detailed, actionable document outlining procedures for identifying, analyzing, containing, eradicating, and recovering from various types of security incidents. This plan is regularly reviewed and updated based on lessons learned and evolving threat landscapes.
* Playbooks - Specific, step-by-step guides for responding to common incident types like malware infection, phishing attacks, denial-of-service attacks, and data breaches.
* Training and Drills - Regular tabletop exercises and simulated incident drills are conducted to test the effectiveness of the IRP and the readiness of the CSIRT. These exercises help identify gaps and improve response times.
* Tooling and Technology - We invest in and maintain advanced security tools, including Security Information and Event Management (SIEM) systems, intrusion detection/prevention systems (IDPS), endpoint detection and response (EDR) solutions, and forensic analysis tools.

**System and Data Identification**

Accurate identification of systems and data is fundamental to effective incident response:

* Asset Inventory - Maintaining a comprehensive and up-to-date inventory of all hardware, software, and network assets. This includes critical servers, workstations, cloud instances, applications, and databases.
* Data Classification - Implementing a data classification policy that categorizes data based on its sensitivity, value, and regulatory requirements whether it be public, internal, confidential, or restricted. This allows for prioritized protection and targeted response efforts.
* Critical Asset Mapping - Identifying critical systems and the data they process, store, or transmit. This mapping helps in understanding the potential impact of an incident on business operations and in prioritizing recovery efforts.
* Network Segmentation - Implementing network segmentation to isolate critical systems and sensitive data, thereby limiting the lateral movement of threats during an incident.

**Incident Detection and Analysis**

Our CSIRT utilizes a combination of automated tools and manual analysis to detect and analyze incidents:

* Continuous Monitoring - SIEM systems and other security tools provide real-time monitoring of network traffic, system logs, and user activity for suspicious patterns.
* Alert Triage - Security analysts rapidly assess alerts generated by security tools to determine their validity and severity.
* Threat Intelligence - Leveraging threat intelligence feeds to stay informed about emerging threats and vulnerabilities relevant to our industry and systems.

**Containment, Eradication, and Recovery**

Once an incident is identified and analyzed, the CSIRT executes containment, eradication, and recovery strategies based on the pre-defined IRP and playbooks, aiming to restore normal operations as quickly and safely as possible.

**Disaster Recovery**

RC Cybersecurity has implemented a Disaster Recovery Program (DR) to address the recovery of critical IT infrastructure and systems in the event of a disaster or significant disruption. The DR program includes the following components:

* Business Impact Analysis - Identifying critical IT systems and determining their recovery time objectives (RTO) and recovery point objectives (RPO). This analysis helps prioritize recovery efforts based on the impact on business operations.
* Backup and Restoration Procedures - Establishing regular backup schedules for critical data and systems. This includes conducting backups at off-site locations to ensure data redundancy. Restoration procedures are documented and regularly tested to ensure the timely recovery of systems.
* Infrastructure and Hardware Redundancy - Implementing redundant infrastructure components, such as servers, storage, and networking equipment, to minimize single points of failure. This ensures that critical systems can be quickly restored in case of hardware failures.
* Testing and Training - Conducting regular tests and drills to validate the effectiveness of the disaster recovery plan. This includes simulating different disaster scenarios and evaluating the organization's ability to recover systems and operations. Training programs are provided to relevant staff members to ensure they are familiar with their roles and responsibilities during a recovery situation.
* Continuous Improvement - Periodic review and updates of the disaster recovery plan based on lessons learned from testing, changes in technology, and evolving business requirements. This ensures that the plan remains relevant and effective over time.

By having a robust Business Continuity Plan (BCP) and Disaster Recovery Program (DR) in place, RC Cybersecurity aims to minimize the impact of disruptions, protect patient care, and maintain operational resilience during unforeseen events.

**References:**

Ballejos, L. (2022, December 16). *Patch Management Audit Checklist | NinjaOne*. Www.ninjaone.com. https://www.ninjaone.com/blog/patch-management-audit-checklist/

Burnard, K., & Bhamra, R. (2011). Organisational resilience: development of a conceptual framework for organisational responses. *International Journal of Production Research*, *49*(18), 5581–5599. https://doi.org/10.1080/00207543.2011.563827

InfoSec. (n.d.). *InfoSec Policy – The Basis for Effective Security Programs*. What-When-How.com. http://what-when-how.com/information-science-and-technology/infosec-policy-the-basis-for-effective-security-programs/

KirkpatrickPrice. (2021, March 29). *The Main Types of Security Policies in Cybersecurity | KirkpatrickPrice*. KirkpatrickPrice Home. https://kirkpatrickprice.com/blog/main-types-security-policies-cybersecurity/

Palo Alto Networks. (2015). *What Is a Next-Generation Firewall (NGFW)? A Complete Guide*. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-next-generation-firewall-ngfw

Palo Alto Networks. (2024). *What is SOAR?* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-soar

Rezaei Soufi, H., Torabi, S. A., & Sahebjamnia, N. (2018). Developing a novel quantitative framework for business continuity planning. *International Journal of Production Research*, *57*(3), 779–800. https://doi.org/10.1080/00207543.2018.1483586

SecurityOrb. (2014, December 20). *The Three General Categories of Policies | SecurityOrb.com*. Securityorb.com. https://securityorb.com/general-security/three-general-categories-policies/

SentinelOne. (2024, August 8). *What is an Incident Response?* SentinelOne. https://www.sentinelone.com/cybersecurity-101/services/what-is-an-incident-response/

Thiyagaraj, R. (2021, August 7). *Business Continuity Planning*. WallStreetMojo. https://www.wallstreetmojo.com/business-continuity-planning/