>_ TASK-1 SUBMISSION

MAIN CRAFT TECHNOLOGIES

STATUS: SECURE

VIRTUAL INTERNSHIP PROGRAM

Cybersecurity Threat Intelligence

Report 2024-2025

A comprehensive analysis of major modern cyber threats, impact assessments, and strategic defense mechanisms for the evolving digital landscape.

PREPARED BY	ROLE	SUBMISSION DATE
VENKAT THOSHISH KRISHNA	Cybersecurity Analyst Intern	January 14, 2025

INDEX // 01-10

Table of Contents

This report navigates through the modern cybersecurity landscape, analyzing critical threats, real-world impacts, and strategic defense mechanisms for 2024–2025.

```
const reportConfig = {
  target: "All Systems",
  status: "Critical",
  modules: [10]
};
// Initializing sequence...
```

SECTION 01

Introduction to Cybersecurity

What is Cybersecurity?

The practice of protecting systems, networks, and data from digital attacks. It encompasses technologies, processes, and controls designed to safeguard against unauthorized access, theft, or damage.

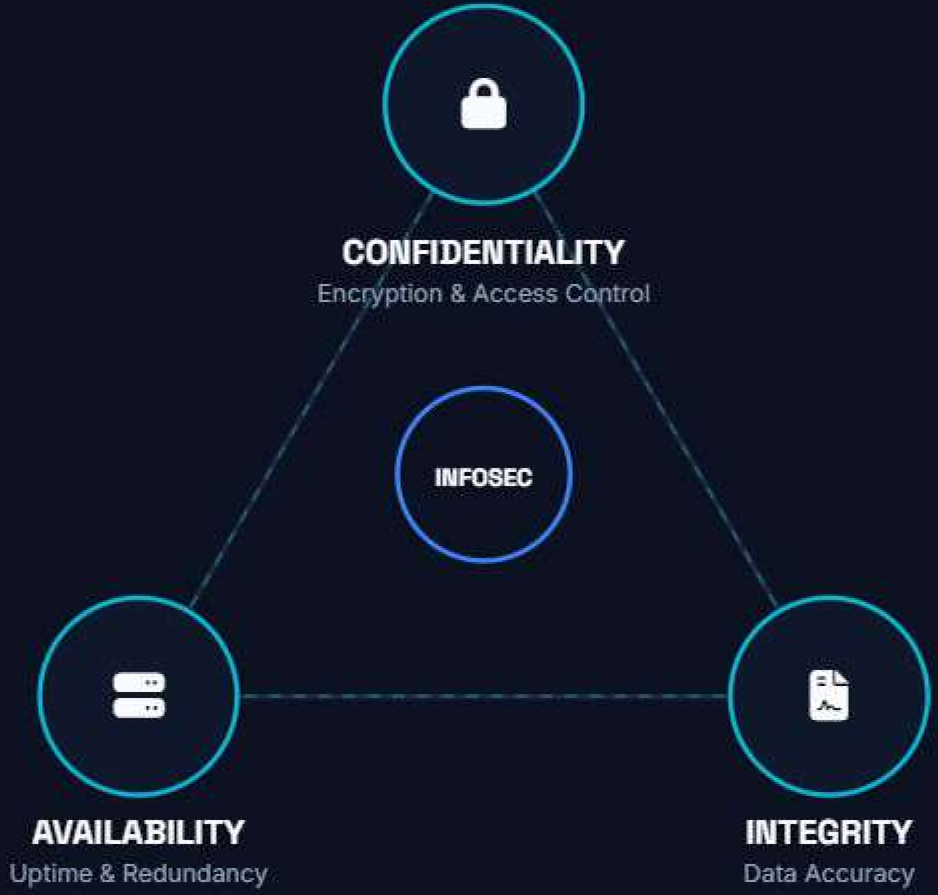
Why it Matters

Prevent Financial Loss	Ensure Business Continuity
Protect Reputation	Legal Compliance (GDPR)

Current Relevance (2024–2025)

Rapid cloud adoption, remote work culture, and AI-driven threats have expanded the attack surface.

> *"Cybercrime is no longer random—it is organized, automated, and profit-driven."*



CONFIDENTIALITY
Encryption & Access Control

INFOSEC

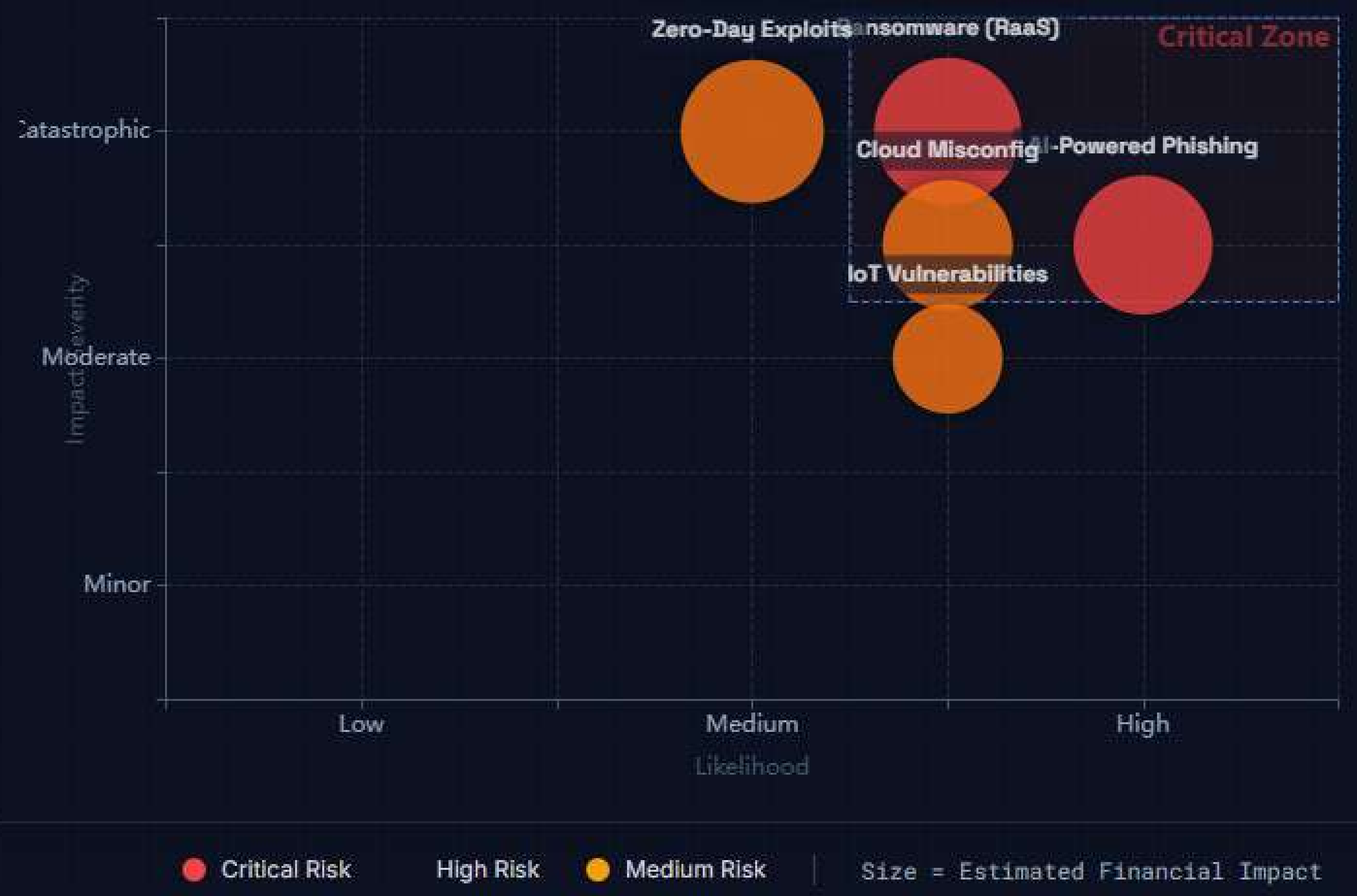
AVAILABILITY
Uptime & Redundancy

INTEGRITY
Data Accuracy

SECTION 02

Threat Landscape Overview 2024-2025

RISK MATRIX ANALYSIS



Primary Targets

- Financial Services & Banking
- Healthcare & Biotech
- Government & Public Sector
- Critical Infrastructure

2025 Trends

AI-DRIVEN ATTACKS	+300%
RANSOMWARE PAYOUTS	+85%

Note: Attackers are shifting from manual hacking to automated, scalable models using Initial Access Brokers (IABs).

SECTION 03

AI-Powered Phishing Attacks

THREAT LEVEL: CRITICAL

Threat Description

AI-powered phishing utilizes **machine learning**, **NLP**, and **deepfake technology** to automate the creation of highly convincing scam emails, voice calls (vishing), and videos. Unlike traditional phishing, these attacks adapt to the target's behavior and writing style.

Impact Analysis

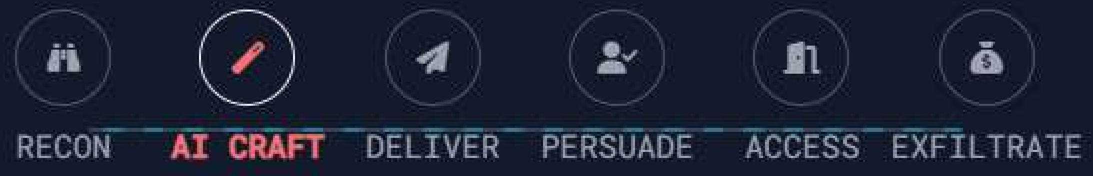
Individuals

- Credential theft
- Financial fraud
- Identity misuse

Organizations

- Unauthorized access
- Massive data breaches
- Loss of trust & reputation

ATTACK KILL CHAIN



Key Differentiator: AI automates the "Craft" and "Persuade" phases with deepfakes and personalized context.

CASE STUDY 2024 **Deepfake CEO Voice Attack**

Several multinational companies reported incidents where attackers used **AI voice cloning** to impersonate CEOs on phone calls.

> $ *"Finance teams were convinced to transfer millions of dollars to fraudulent accounts, believing they were following direct urgent orders from executive leadership."*

Preventive Measures

- ✓ Phishing-Resistant MFA (FIDO2)
- ✓ Out-of-Band Verification
- ✓ AI-Based Email Filtering
- ✓ Employee Awareness Training

Recommended Implementation Priority: High

SECTION 04

Ransomware-as-a-Service (RaaS)

THREAT LEVEL: CRITICAL

Threat Description

RaaS is a business model where malware developers sell or rent ransomware tools to **"affiliates"** (hackers). Affiliates execute attacks without needing deep technical skills, splitting ransom profits with the developers. This has industrialized cybercrime.

Impact Analysis

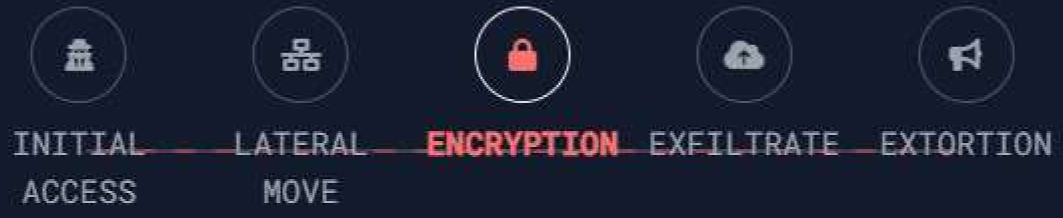
Individuals

- Permanent data loss
- Personal extortion
- Device lockout

Organizations

- Operational shutdown
- Double extortion (Leak)
- Compliance penalties

RaaS KILL CHAIN



INITIAL ACCESS → LATERAL MOVE → ENCRYPTION → EXFILTRATE → EXTORTION

Evolution: Modern RaaS groups (e.g., LockBit) use "Double Extortion" — encrypting data AND threatening to publish it.

CASE STUDY 2017 WannaCry Ransomware

A global attack exploiting the **EternalBlue** vulnerability in unpatched Windows systems. It impacted 200,000+ computers across 150 countries.

> *"The UK's National Health Service (NHS) was severely crippled, leading to cancelled surgeries and diverted ambulances due to locked systems."*

Preventive Measures

- ✓ Offline Backups (3-2-1)
- ✓ Patch Management
- ✓ Endpoint Detection (EDR)
- ✓ Network Segmentation

Recommended Implementation Priority: Critical

SECTION 05

Cloud Security Misconfigurations

⚠ THREAT LEVEL: HIGH

Threat Description

Cloud misconfigurations occur when storage buckets, databases, or services are left publicly accessible due to improper IAM policies, network settings, or default configurations. This is often the result of human error rather than sophisticated hacking.

Impact Analysis

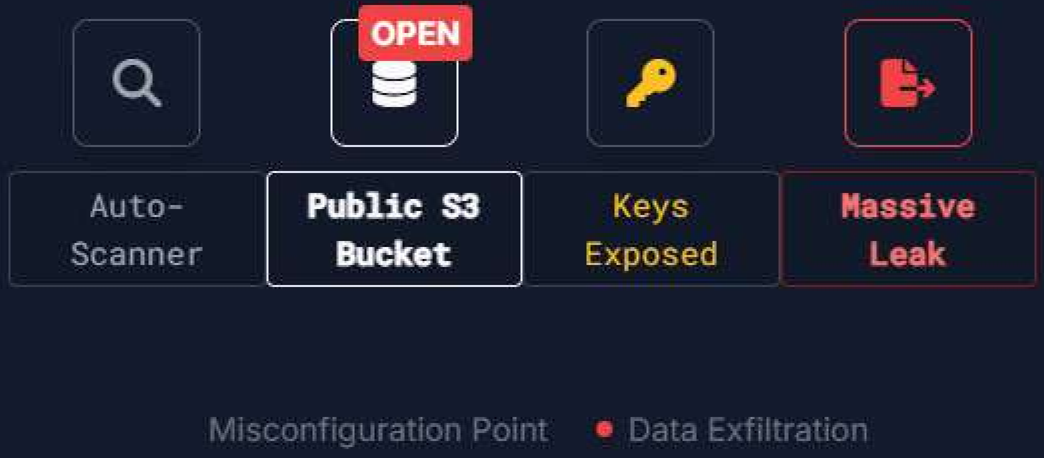
Individuals

- Exposure of PII data
- Privacy violations
- Identity theft risk

Organizations

- Massive data leaks
- GDPR/HIPAA fines
- Regulatory penalties

ATTACK PATH VISUALIZATION



CASE STUDY 2019 Capital One Data Breach

A misconfigured Web Application Firewall (WAF) allowed an attacker to perform a Server-Side Request Forgery (SSRF) attack, accessing AWS S3 buckets.

> *"Over 100 million customer records were exposed, including credit scores, balances, and social security numbers, leading to an $80 million fine."*

Preventive Measures

- ✓ CSPM Tools
- ✓ Regular Audits
- ✓ Least Privilege (IAM)
- ✓ Drift Detection

Recommended Implementation Priority: Critical

SECTION 06

IoT Vulnerabilities

THREAT LEVEL: HIGH

Threat Description

Internet of Things (IoT) devices often lack robust security controls. Issues like **hardcoded default passwords**, outdated firmware, and unencrypted protocols make them easy entry points for attackers to infiltrate deeper into networks.

Impact Analysis

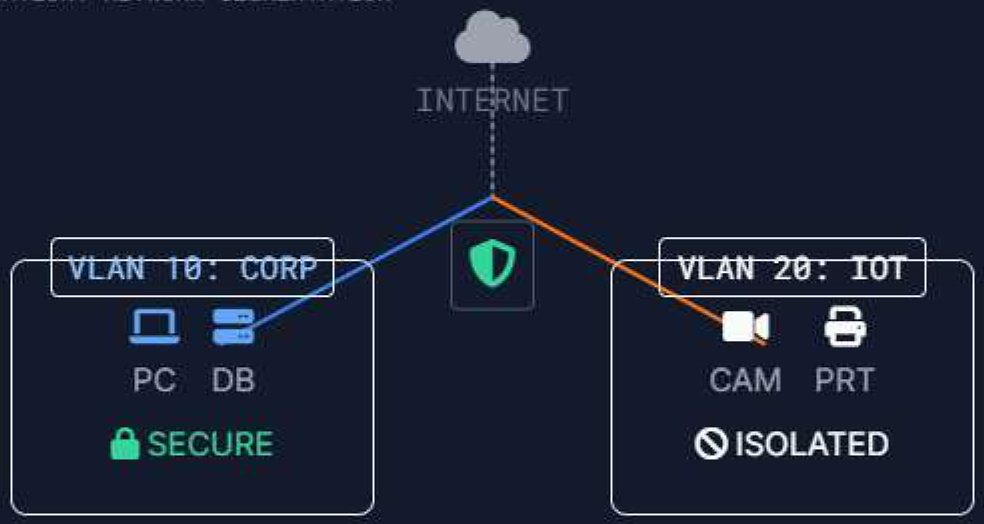
Individuals

- Privacy invasion (Cameras)
- Digital surveillance
- Device hijacking

Organizations

- Massive Botnets (DDoS)
- Pivot to Corp Network
- Operational Disruption

MITIGATION: NETWORK SEGMENTATION



CASE STUDY Mirai Botnet

The Mirai malware scanned the internet for IoT devices using 60 common **default username/password** combinations (e.g., admin/admin), enslaving huge numbers of cameras and routers.

> ⚡ *"Resulted in massive DDoS attacks (1+ Tbps) that took down major services like Twitter, Netflix, and Reddit by overwhelming DynDNS infrastructure."*

Preventive Measures

- ✓ Network Segmentation
- ✓ Disable UPnP
- ✓ Change Default Creds
- ✓ Regular Firmware Updates

Defense Priority: Medium-High

SECTION 07

Zero-Day Exploits

THREAT LEVEL: HIGH

Threat Description

Zero-day exploits target vulnerabilities that are **unknown to the vendor** and have no patch available. These are highly prized by **Advanced Persistent Threats (APTs)** and state-sponsored actors for stealthy, long-term espionage campaigns.

Impact Analysis

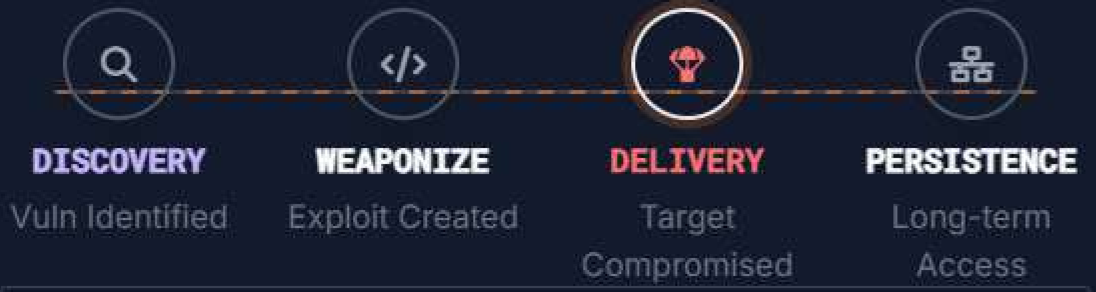
Individuals

- Silent compromise
- Data theft without alerts
- Device botnet recruitment

Organizations

- Long-term espionage
- Intellectual property theft
- Severe data breaches

EXPLOIT LIFECYCLE



DISCOVERY
Vuln Identified

WEAPONIZE
Exploit Created

DELIVERY
Target Compromised

PERSISTENCE
Long-term Access

Challenge: Zero "Detection" days available before attack launch.

CASE STUDY 2020 SolarWinds Supply Chain Attack

Attackers inserted malicious code into the **Orion** software updates. Because the update was digitally signed by a trusted vendor, it bypassed traditional defenses.

> *"Compromised 18,000 organizations worldwide, including US government agencies, remaining undetected for months."*

Strategic Defense

- ✓ Zero Trust Architecture
- ✓ Behavioral Analytics
- ✓ Virtual Patching (WAF/IPS)
- ✓ Threat Intelligence Feeds

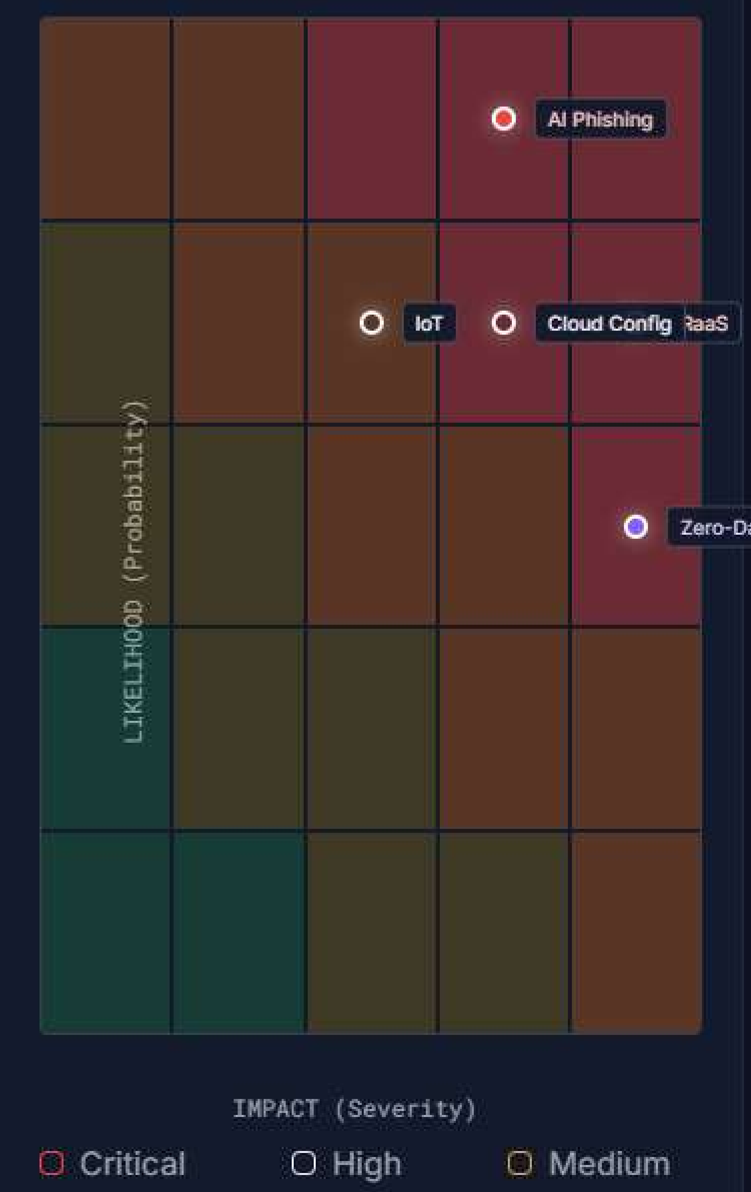
Defense Maturity Required: Advanced

SECTION 08

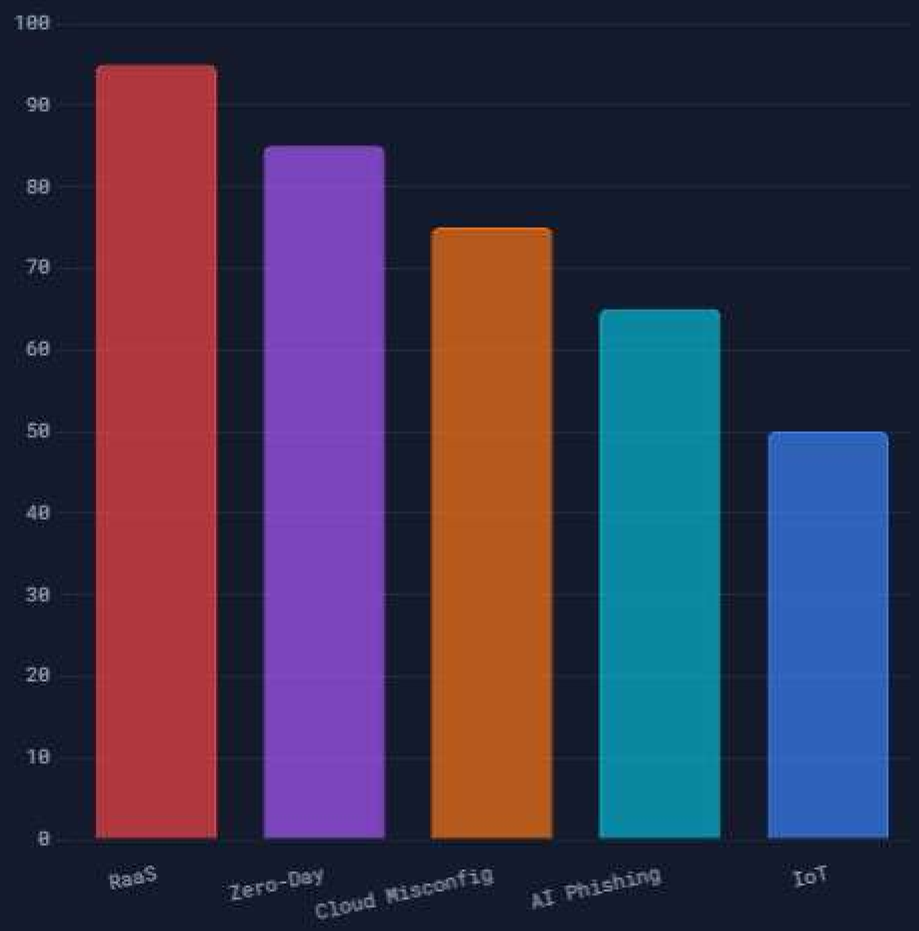
Impact Analysis Summary

DATA VISUALIZATION

▦ Risk Heatmap

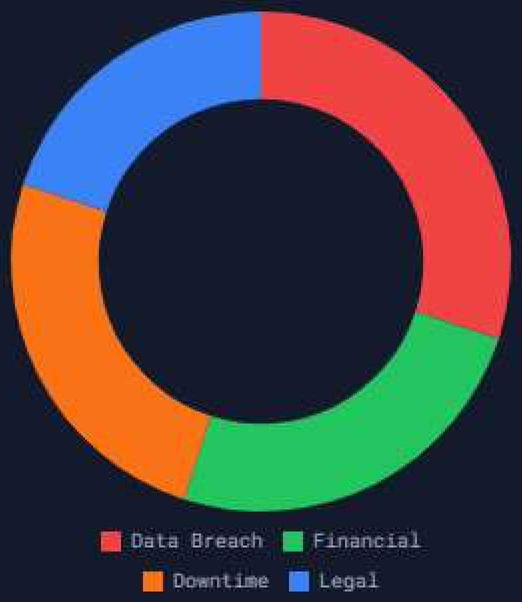


⚖ Estimated Business Impact



ⓘ **Analysis:** RaaS poses the highest immediate financial risk due to ransom demands and operational paralysis. Zero-day exploits have high strategic impact but lower frequency.

Affected Domains



Critical Insights

TIME-TO-DETECT
Avg. 212 days for data breaches vs. minutes for ransomware encryption.

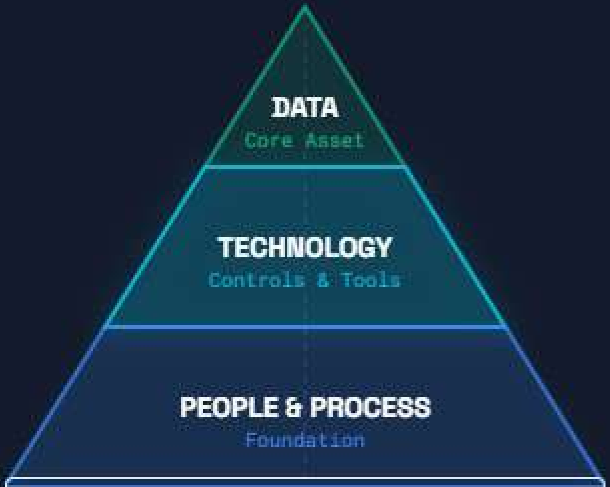
INDIRECT COSTS
Legal fees & reputation damage often exceed technical recovery costs by 3x.

SECTION 09

Preventive Measures – Best Practices

STRATEGY: DEFENSE-IN-DEPTH

Defense Layers



No single layer is sufficient. Security requires overlapping controls.

People

- ✓ Security awareness training (quarterly)
- ✓ Simulated phishing drills & reporting
- ✓ Role-based access reviews

Process

- ✓ Patch SLAs (Critical ≤ 7 days)
- ✓ Strict Change Control Board (CCB)
- ✓ Incident Response (IR) Playbooks

Technology

- ✓ MFA everywhere (Phishing-resistant)
- ✓ EDR/XDR on all endpoints
- ✓ Immutable & Offline Backups
- ✓ Zero Trust Network Access (ZTNA)

Data

- ✓ Data Classification & Tagging
- ✓ Encryption at Rest & in Transit
- ✓ Data Loss Prevention (DLP) rules

Monitoring & Visibility

- ✓ Centralized Logging (SIEM)
- ✓ User Behavior Analytics (UEBA)
- ✓ Continuous Compliance Monitoring

SECTION 10

Conclusion & Future Scope

FINAL SUMMARY

The Paradigm Shift: From Reactive to Proactive

Cybersecurity threats are evolving faster than ever, driven by AI automation and organized crime. Organizations can no longer rely on defending the perimeter. **Resilience** requires a layered, data-driven approach where security is baked into every process, not bolted on at the end.

SECURE BY DESIGN

Secure AI/LLM

Governance for AI adoption and defense against adversarial machine learning attacks.

Zero Trust

Identity-first security model: "Never trust, always verify" for every access request.

Supply Chain

Rigorous vetting of third-party vendors and Software Bill of Materials (SBOM).

Cloud Native

Automated guardrails and Policy-as-Code for multi-cloud environments.

Path for Professionals

Cybersecurity is a journey of lifelong learning. Stay curious, practice in home labs, follow threat intelligence feeds, and contribute to the community. The attackers never stop learning, so neither should we.

THANK YOU

"Secure by design. Measurable by metrics."