Borderless CS
CYBER SAFE TOGETHER

Building Digital Shift:

The Strategic Importance of Cybersecurity Principles in a Connected Pacific

Presented By:

Jayaprakash (JP) MUTHUSAMY

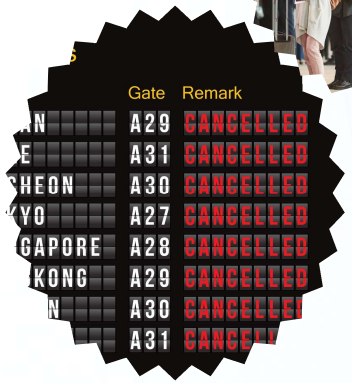
CEO & Director of Cybersecurity Practice

Borderless CS

https://borderlesscs.com.fj

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International



When Leadership Overlooked Security:

What will happen

- **July 2025:** Russia's largest airline grounded due to Cyberattack
- Dozens of flights canceled, nationwide disruption, passenger chaos
- Investigation revealed **CEO had not changed password since 2022 —** a simple oversight with huge consequences

What if this happened to Pacific critical services—airlines, ports, or telecoms?

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

IS PACIFIC LEADERSHIP CYBER-READY?

- How often are executive credentials updated in your organisation?
- If a cyberattack struck tomorrow, could operations continue?
- Do leaders truly understand their cyber risk exposure?

"Cyber resilience starts in the boardroom."

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

PACIFIC DIGITAL SHIFT - OPPURTUNITIES AND RISING CYBER RISK

Digital Opportunity

Digital transformation projected to add **US $5B to GDP by 2040**

Approx. 300K ICT jobs projected across Pacific SIDS

79% internet users in Fiji; strong 3G/4G coverage

Mobile connections: 152% of population

Cyber Risks

34% of global cyberattacks targeted Asia-Pacific (2024)

Over **20% of APT** attacks focused on APAC nations

Global cybercrime costs projected to hit **US $23T by 2027**

Pacific governments & businesses already experiencing **targeted phishing and ransomware**

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

CYBERCRIME LANDSCAPE & ITS IMPACT ON THE PACIFIC

31% of global cyberattacks target Asia-Pacific

Phishing & Credential Theft

Top reported threat in Pacific Island CERT data

Ransomware & Malware

Rising incidents across APAC businesses

Organized Fraud (Scams & BEC)

- Mobile-money fraud (“m-paisa” scams in Fiji)
- Online shopping cons on the rise

Government & Telecom Targets

- Attacks on Vanuatu’s networks
- Marshall Islands telecom breach

💰 **Global Cybercrime Losses: $9.5 Trillion (2024) |** ⚠️ **“20% of APT attacks focus on APAC nations”**

Sources: forumsec.org | pacson.org | production-new-commonwealth-files.s3.eu-west-2.amazonaws.com

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

BRIDGING THE DIGITAL DIVIDE FOR CYBER RESILIENCE

86% Mobile Broadband Coverage

High connectivity

Only 27% actively use mobile internet

Digital usage gap: 59%

Usage Gap

Few trained Cybersecurity staff

Cybersecurity readiness Gap

Connectivity alone isn't enough – readiness is key to resilience.

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

2025 – CYBER ATTACKS OVERVIEW

Borderless CS
CYBER SAFE TOGETHER

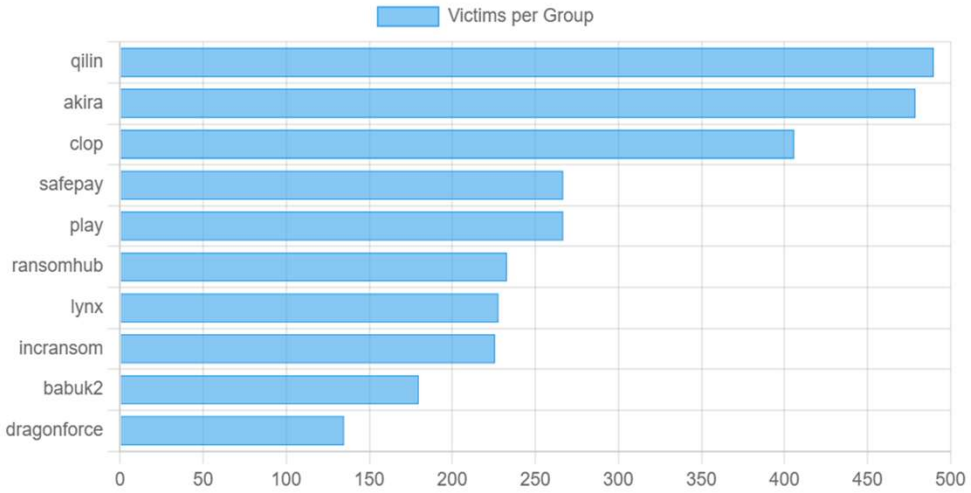
ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

Ransomware Statistics for 2025

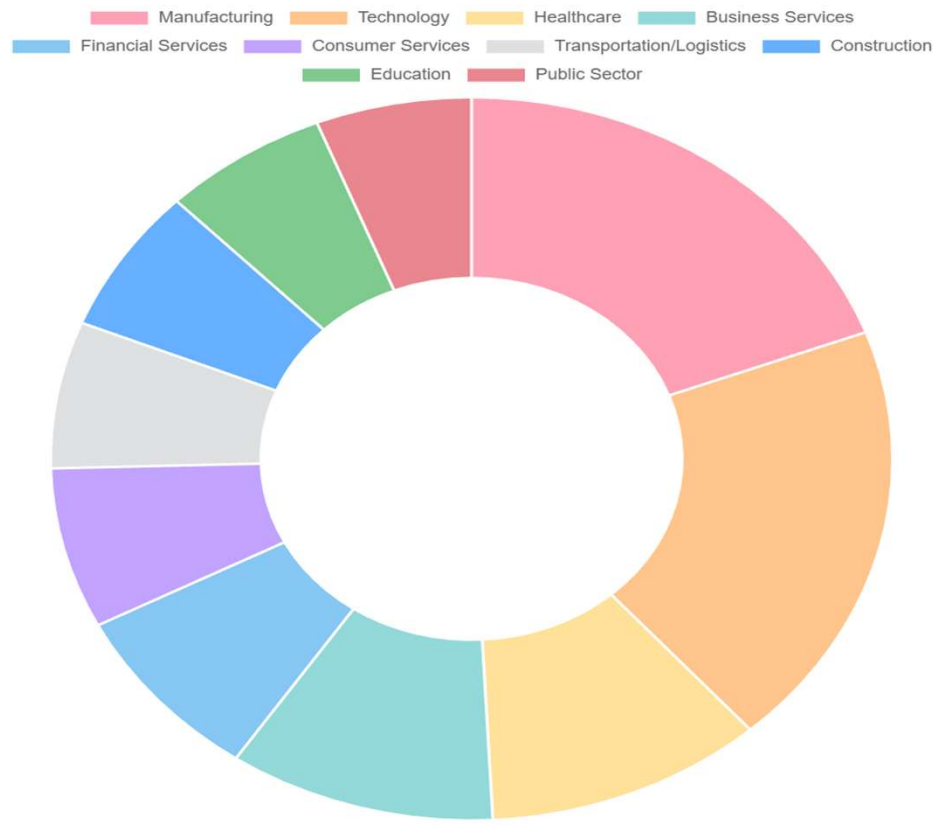
Total Victims for 2025: 5213

Total Groups: 286

Top 10 Groups



Top 10 Sectors



2024 – CYBER ATTACKS OVERVIEW

Did you know?

- In 2024, 16.3% of organizations that were hit by ransomware were forced to pay ransoms to recover their data (up from 6.9% in 2023).
- Ransomware payments skyrocketed to record highs, with total payments of $459.8 million.
- The average ransom demand per attack exceeded $5.2 million in just H1 2024.
- The average attack cost was $4.91 million, making ransomware the third-costliest cyberattack of 2024.
- 46% of security professionals estimate that their organizations suffered losses of $1-10 million in terms of ransom fees, lost revenues, and brand damage.
- 78% of organizations attacked in 2023 were breached again in 2024; 63% of these were asked to pay even higher ransoms the second time.
- In 2024, 56% of attacked organizations didn't detect a ransomware breach for 3-12 months, indicating a low level of awareness and preparedness to this threat.
- Also, only 22% of attacked organizations recovered from an attack within a week, indicating a worrying increase in recovery times.
- Organizations with good cybersecurity hygiene have a 35X lower frequency of experiencing destructive ransomware events, which shows that hygiene plays an important role in reducing the impact of ransomware attacks.

Living-Off-the-Land (LOTL) Attacks:

Living off the land (LOTL) is a fileless malware or LOLbins cyberattack technique where the cybercriminal uses native, legitimate tools within the victim's system to sustain and advance an attack.

REGIONAL COOPERATION & INITIATIVES

- **PaCSON (Pacific Cyber Security Operational Network):**
  - **Regional incident response & info sharing** (16 PICs plus Australia and New Zealand as partners)
- **Pacific Fusion Centre:**
  - Strategic **threat intelligence** and policy support
- **Public awareness campaigns**:
  - "Cyber Smart Pacific"
  - "Cyber Safety Pasifika"
- **Diplomatic frameworks** embed cybersecurity priorities:
  - 2023 Lagatoi Declaration commits to s**ecure digital transformation**
  - 2050 Blue Pacific Continent Strategy prioritizes **cyber resilience**

Sources: forumsec.org | pacson.org | digitaldevelopment.org | itu.int | dfat.gov.au | publicadministration.un.org

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

THE STRATEGIC SHIELD

5 PRINCIPLES FOR PACIFIC LEADERS

Risk Management
Identify, assess, and mitigate cyber threats

Resilience
Design systems to withstand and recover from attacks

Accountability
Embed responsibility across all levels

Innovation
Treat security as an enabler, not a barrier

Governance
Leadership-driven policies and accountability

🔑 "**81%** of breaches caused by **weak/reused passwords**"

⏱️ "**207 days** — average breach detection time globally"

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

REAL-WORLD CYBERSECURITY LESSONS: USE CASES

1

Qantas Call Centre Hack: 6 Million Customers Exposed

2

Metricon Homes Ransomware Attack

3

Tea App Social Engineering Scam

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

Qantas Call Centre Hack: 6 Million Customers Exposed

How the Manila Contact Centre Hack Happened

Attacker Preparation
AI-generated **voice deepfake** created to impersonate IT staff

Social Engineering Attack
Deepfake call to helpdesk requesting credential reset

Credential Reset
Helpdesk **resets credentials**, **bypassing MFA**

Platform Access & Data Theft
Hackers access third-party platform, steal sensitive customer data

Impact
Up to 6 million customers' personal data exposed

How It Worked

Impersonation method: Possibly AI-generated voice deepfakes
Attack vector: Convinced helpdesk to reset credentials, bypassing MFA
Suspected group: Scattered Spider — known for advanced impersonation tactics

REAL-WORLD CYBERSECURITY LESSONS: USE CASES

1

Qantas Call Centre Hack: 6 Million Customers Exposed

2

Metricon Homes Ransomware Attack

3

Tea App Social Engineering Scam

Metricon Homes Ransomware Attack: 128GB of sensitive data

What Happened

- The **Qilin ransomware group** claimed responsibility for attacking Metricon Homes.
- **128GB of sensitive data exfiltrated,** including:
  - Financial documents
  - Architectural plans
  - HR records

How It Worked

- Likely **entry via phishing or spear phishing emails**, a common tactic used by Qilin.
- Once inside, attackers **deployed Agenda ransomware**,
  - **Encrypted systems**
  - **Threatened to leak data** on the dark web

REAL-WORLD CYBERSECURITY LESSONS: USE CASES

Qantas Call Centre Hack: 6 Million Customers Exposed

Metricon Homes Ransomware Attack

Tea App Social Engineering Scam

Tea App Social Engineering Scam: 1.1 million private messages exposed

Breach

The Tea App, designed for women's dating safety, suffered a massive breach exposing 72,000 images and 1.1 million private messages.

Vulnerability

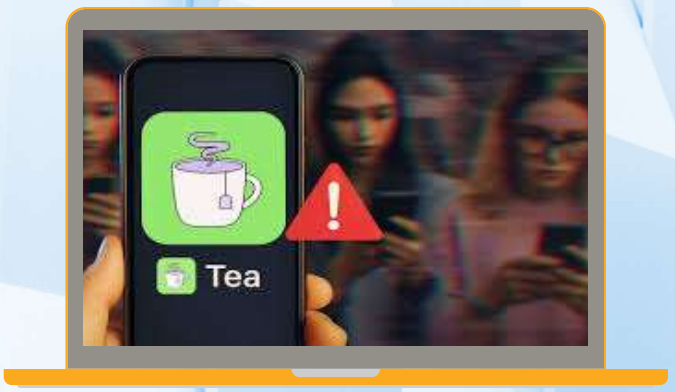
Attackers exploited an **unsecured Firebase database** and used a Python script to download user data.

Exposure

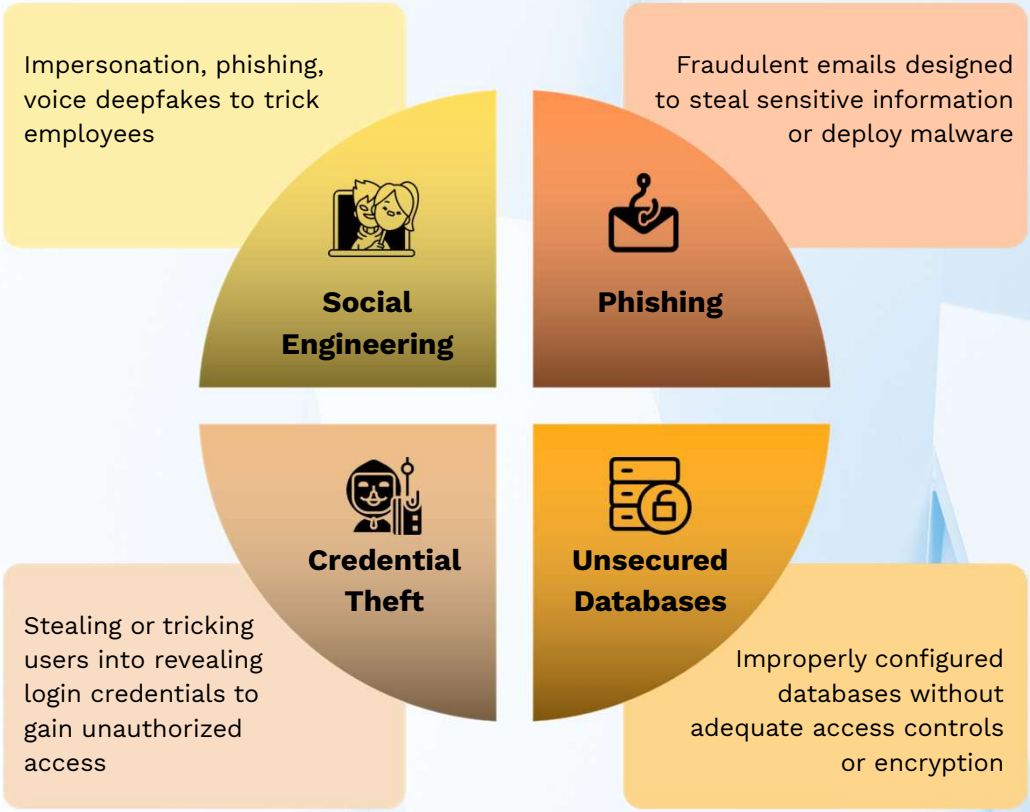
The app stored selfies, government IDs, and DMs **without** proper **encryption or access controls.**

Aftermath

Hackers posted the stolen data on 4chan and created Google Maps overlays to track users' locations.



COMMON ATTACK VECTORS ACROSS THESE BREACHES



Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

BE AWARE OF SCAMS

- ✔ Phishing
- ✔ Vishing – phone call
- ✔ Ransomware Attacks

Look out for :

- Urgency
- Asking for personal/financial information
- Unsolicited Communications
- Contain links and downloadable files
- Bad grammar
- Too good to be true
- Verify Caller Identity

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

HOW TO PREVENT THESE ATTACKS

1. Employee Training

Regularly educate staff to recognize phishing attempts, social engineering tactics, and suspicious behavior.

2. Strong Authentication

Implement multi-factor authentication (MFA) across all critical systems and enforce regular password updates

3. Vendor Risk Management

Continuously assess and monitor third-party providers for security compliance and vulnerabilities.

4. Network Monitoring & Incident Response

Deploy tools to detect unusual activity early and establish a clear, practiced incident response plan.

5. Data Protection

Encrypt sensitive data at rest and in transit, and maintain secure, frequent backups to enable recovery.

6. Zero Trust Security Model

Adopt a “never trust, always verify” stance, requiring strict access controls for all users and devices.

7. Patch and Update Management

Regularly apply software patches and updates to close security gaps and protect against known vulnerabilities.

8. Access Controls & Least Privilege

Limit user and system permissions strictly to what is necessary to reduce potential attack surfaces.

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

UNITED AGAINST INVISIBLE THREATS

REGIONAL TRUST IS OUR GREATEST DEFENSE

- **Cyber threats don't respect borders** – Attacks in one nation ripple across the region
- **Shared frameworks & real-time threat sharing** strengthen collective defense
- **Communities as frontline defenders** – Awareness and training are our shield
- **70% of Pacific Island nations lack response plans**, leaving major vulnerabilities
- **Trust and collaboration** transform threats into manageable challenges

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

CYBER RESILIENT PACIFIC

Governments

- Policies, national CERTs, cyber laws
- Secure digital infrastructure

Businesses

- Embed cybersecurity into daily operations
- Reduce ransomware risks

Communities

- Awareness, safe online practices
- Early threat reporting

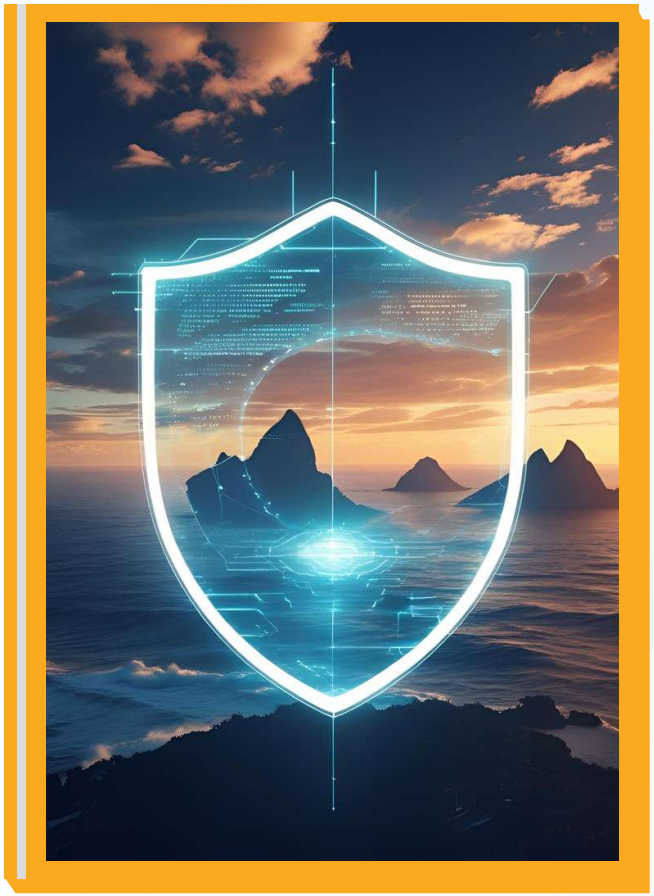
Borderless CS

- Acts as **trusted regional advisor & vCISO**
- **Bridges gaps** between government, business, and communities
- Leads **collaborative frameworks** and cyber resilience initiatives

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International



CALL TO ACTION

SECURE THE DIGITAL FUTURE OF THE PACIFIC

- **Embed Cybersecurity Principles**: Start early in all digital initiatives and maintain continuous vigilance.
- **Leadership Accountability**: Build a risk-aware culture where boards and executives own cyber resilience.
- **Regional Collaboration**: Unite Pacific nations and organizations to strengthen digital ecosystems.
- **Partner With Us:** Work together to create a secure, sustainable digital future.

The Pacific's digital future is bright—let's secure it together.

contact@borderlesscs.com.fj https://borderlesscs.com.fj +679 949 0464

Borderless CS
CYBER SAFE TOGETHER

ISO 27001| ISO 9001 | ISO 45001 | GDPR | SOC 2 Type II | CREST ANZ | CREST International

Your Questions, Our Commitment

More Information

info@borderlesscs.com.fj
info@borderlesscs.com.au

1300 854 340
+679 949 0464

https://borderlesscs.com.fj
https://borderlesscs.com.au