



THE LATEST RANSOMWARE ATTACK TRENDS AND TECHNIQUES

A N D A C T I O N A B L E S T R A T E G I E S T O C O M B A T
M O D E R N R A N S O M W A R E T H R E A T S

Presented by: Venishan Naidu (CISA), (CGEIT), (CDPSE), (CISSP)



“South African ranked number one in Africa, for ransomware and infostealer attacks in the second half of 2024 - ESET bi-annual Threat Report.”

ICT GOVERNANCE AND WHY IT MATTERS FOR RANSOMWARE DEFENSE

- 🚫 **Risk Management:** Identifies and mitigates ransomware risks proactively.
- 🚫 **Accountability:** Defines roles and responsibilities for cybersecurity.
- 🚫 **Compliance:** Ensures adherence to legal and regulatory standards (e.g., POPIA, GDPR).
- 🚫 **Resilience:** Builds a culture of preparedness and rapid response.



KEY IT GOVERNANCE FRAMEWORKS



- COBIT: Focuses on aligning IT with business goals and managing risk.
- ISO/IEC 27001: Provides a framework for an Information Security Management System (ISMS).
- NIST Cybersecurity Framework: Offers guidance on identifying, protecting, detecting, responding, and recovering from cyber threats.

POPIA PENALTIES FOR DATA BREACHES (as of 2025)

1. Administrative Fines

Up to R10 million for non-compliance

2. Criminal Sanctions

Up to 10 years' imprisonment for responsible individuals in serious cases

3. Civil Liability

Affected individuals may sue for damages if their personal information was compromised due to negligence

4. Reputational Damage

Loss of consumer trust and brand credibility can have long-term financial consequences.

5. Mandatory Breach Notification

Organizations must report breaches to the Information Regulator and affected individuals, regardless of the breach's severity

RANSOMWARE TRENDS AND TECHNIQUES PREDICTED TO CONTINUE IN 2025

- Specific techniques as opposed to generic/ mass techniques
- Supply chain attacks – large scale commercial software that has one or more vulnerabilities
- Triple Extortion
 - Single – encrypt data, ransom for decryption key
 - Double – movement of data to a separate location
 - Triple – leak data unless Ransom is paid
- Attacks of unpatched systems – zero day, known vulnerabilities, unpatched systems

RANSOMWARE TRENDS AND TECHNIQUES PREDICTED TO CONTINUE IN 2025

- Phishing – inclusion of generative AI
- Generative AI – friend and foe
- Attacks move faster
- Small and medium businesses targeted
- Ransomware as a service
- Cloud Exploits



Strengthening cyber security controls

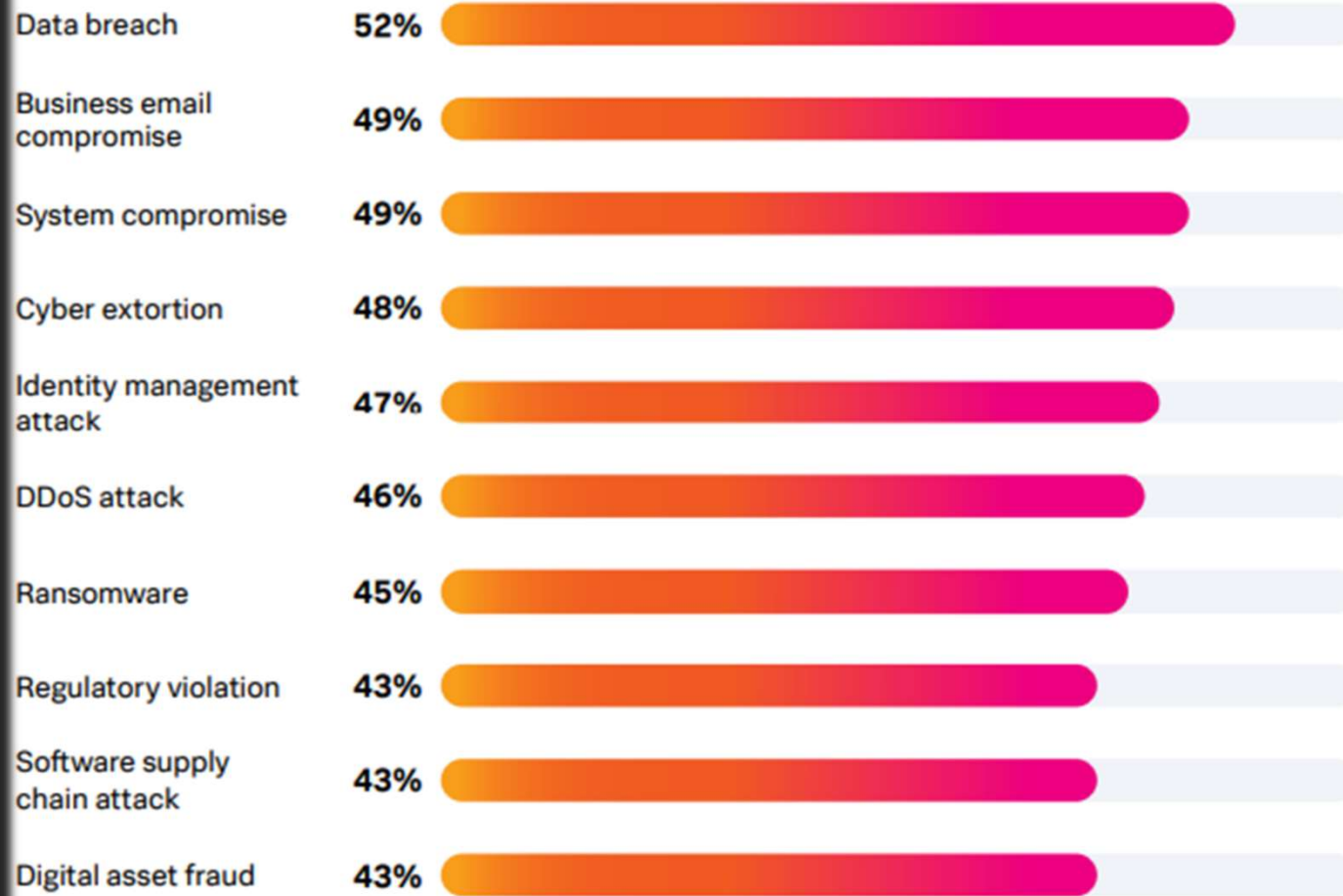
Actionable Strategies to Combat Ransomware

- ICT Governance
- Employee Training and Awareness
- Layered security
- Zero Trust Architecture
- Advanced Protection Technologies - Endpoint Detection & Response (EDR)
- Regular Backups
- Patch Management
- Network Segmentation
- Threat Intelligence Integration
- Continuous monitoring and auditing
- Table Top Exercises

I N C I D E N T R E S P O N S E P L A N N I N G

- Develop and test a ransomware-specific incident response plan
- Include legal, PR, and executive teams in tabletop exercises
- Maintain offline copies of critical response documentation
- Document lessons learnt and corrective action

Most frequent incidents experienced in the past two years



Source: State of Security 2024 | Splunk

CYBERSECURITY VS CYBER RESILIENCE

CYBERSECURITY

Definition: Procedures followed, or measures taken to ensure the safety of a state or an organization

Technologies and process designed to protect an organization from cybercrime

Works to reduce the risk of cyber and to protect the organization from cyber attacks

Can work effectively without compromising the usability of other systems

Includes a business plan to resume operations in the event of a successful attack

CYBER RESILIENCE

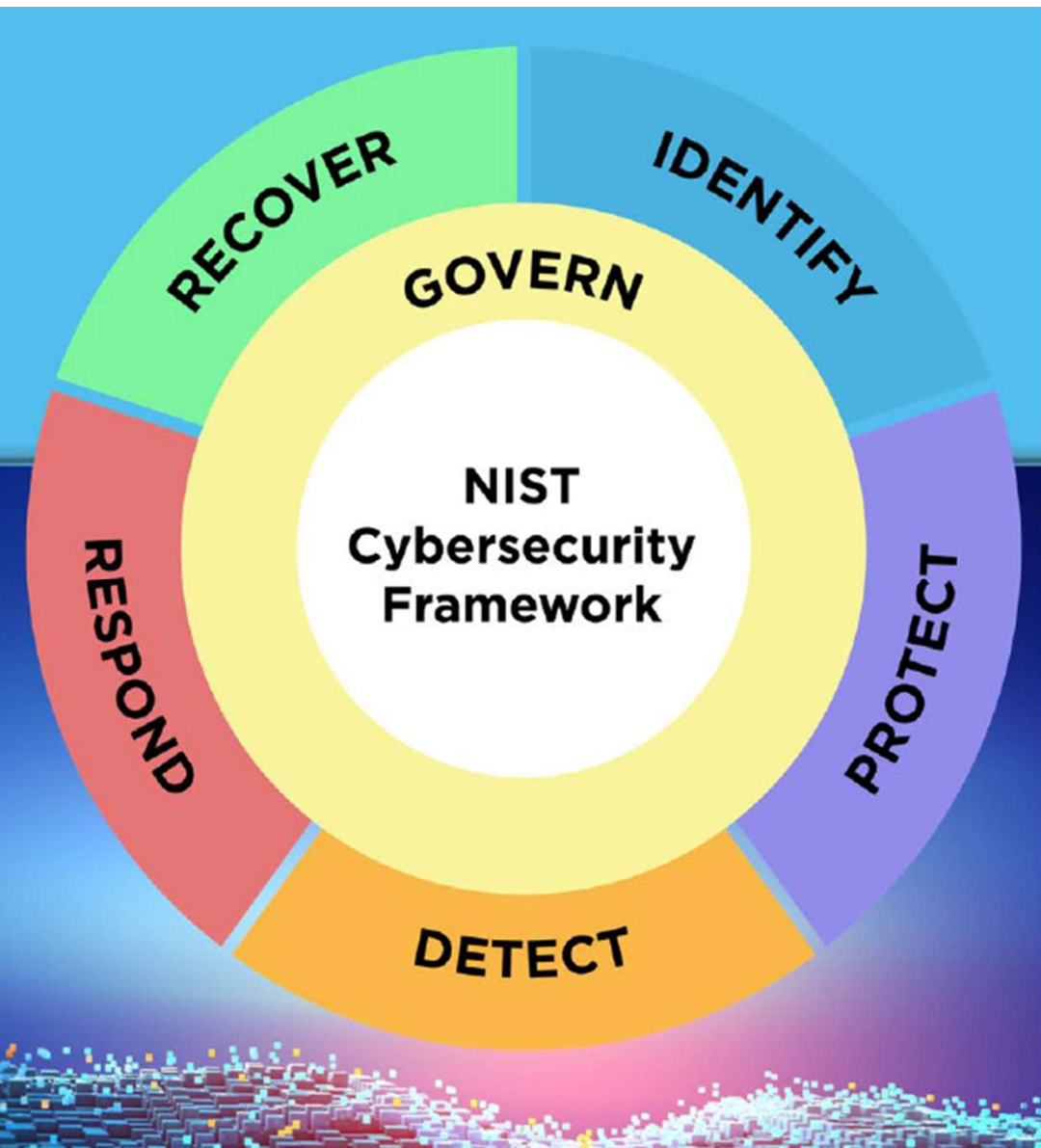
Definition: The capacity to recover quickly from difficulties or toughness

Technologies and processed designed to keep delivering intended services in spite of cyber incidents

Works to ensure continuity on a wider scope comprising cybersecurity and business requirements

Requires organization-wide culture shift that normalizes and embeds security best practices

Requires the organization to become agile and adaptable in the face of cyber attacks and incidents



1. The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
2. The organization's current cybersecurity risks are understood.
3. Safeguards to manage the organization's cybersecurity risks.
4. Possible cybersecurity attacks and compromises are found and analyzed.
5. Actions regarding a detected cybersecurity incidents are taken.
6. Assets and operations affected by a cybersecurity incident are restored.

*This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.29>*

Function	Category	Category Identifier
<u>Govern (GV)</u>	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
<u>Identify (ID)</u>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<u>Protect (PR)</u>	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
<u>Detect (DE)</u>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<u>Respond (RS)</u>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<u>Recover (RC)</u>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Take Aways



Protect

- Patch application & OS
- Block macros in Microsoft office
- Enable MFA
- IT Security policy enforcement



Detect

- Regular vulnerability assessments
- Foster Partnerships and collaboration
- Continuously monitoring threats
- Awareness and Training



Respond

- Develop and Incident response plan
- Maintain BCP and DRP
- Awareness and Training
- Prepare for the eventuality



Recover

- Incident recovery plan
- Sound backup and restoration strategy
- Cyber security insurance
- Third Party Vendor management (SLA)



THANK YOU!

Any Questions?