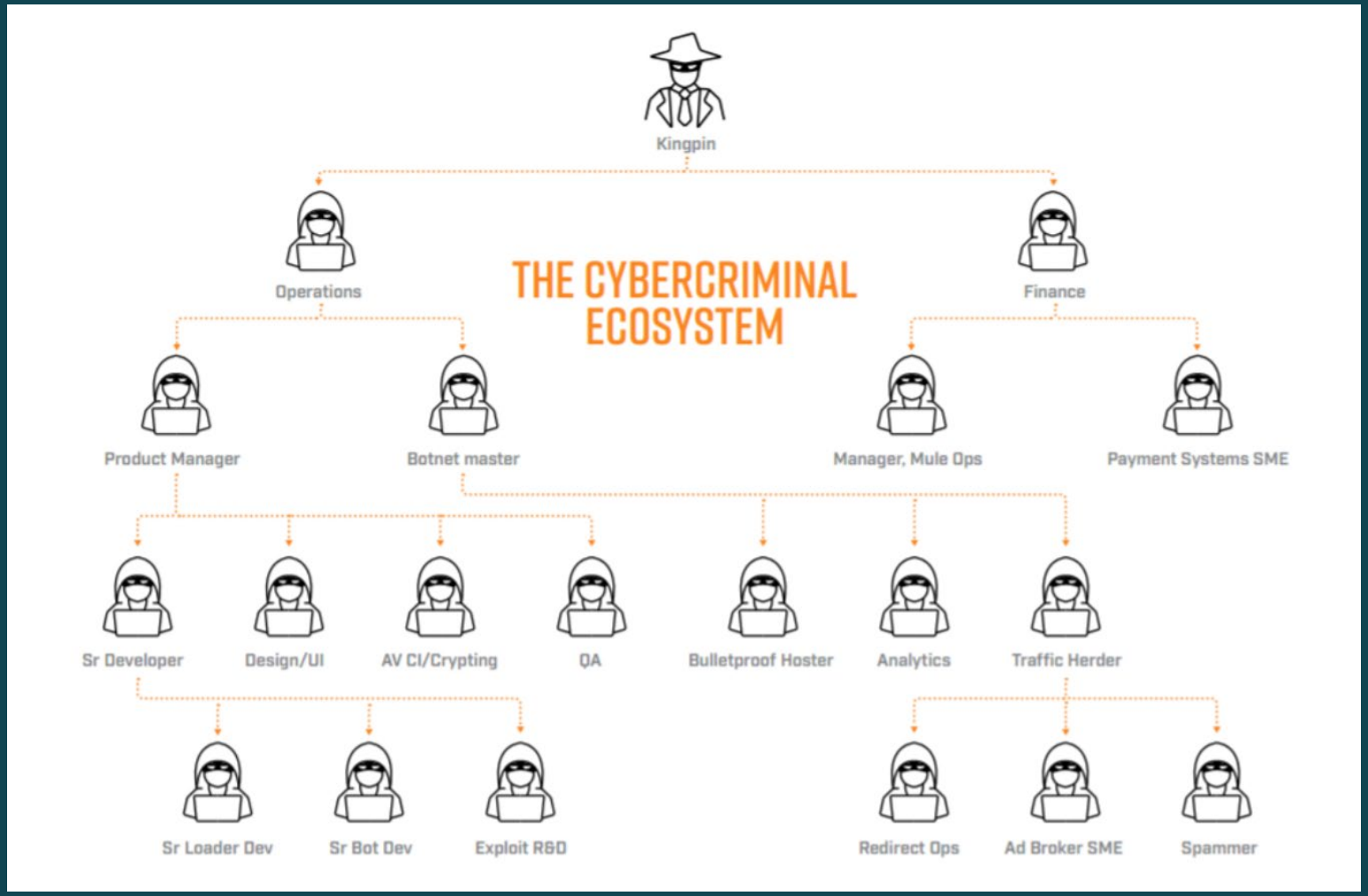
Cybercrime Trends

Presenter : Mauritz Grobler CISM

Cyber Crime



Primary activities

Discover Vulnerabilities → Prepare for exploit → Deliver exploit → Activate Cyber Attack

General Cyber Security Trends

- Cloud facing mobile workforce has changed the IT perimeter.
- Cyber criminals no longer hack into enterprise networks; they target the weakest link “The User” and simply log in using stolen credentials.
- Once inside the target network, criminals expand their attack and move laterally across the network, hunting for privileged accounts and credentials that help them gain access to the organization’s most critical infrastructure and sensitive data.
- Fileless malware makes up over 50% of malware detections rendering traditional protective controls ineffective. 50%+ Unmitigated endpoint risk.
- Attack orchestration has greatly reduced the time organisations have to respond to security incidents. Its time to assume a breach.

Insurance vertical

Insurance companies are known to store large amounts of information about their policyholders.

This practice makes them a target for cybercriminals.

Insurance vertical

Loss of confidential data – Insurers are a high target for criminals because of personally identifiable information that they collect.

Disruption of business – Cyber attacks can disrupt normal business operations and require significant recovery costs.

Reputational damage – Policyholder trust might be compromised in the event of a cyber attack, where confidential information of policyholders is exposed.

Cyber attacks pose a reputational risk that may affect the insurance sector as a whole.

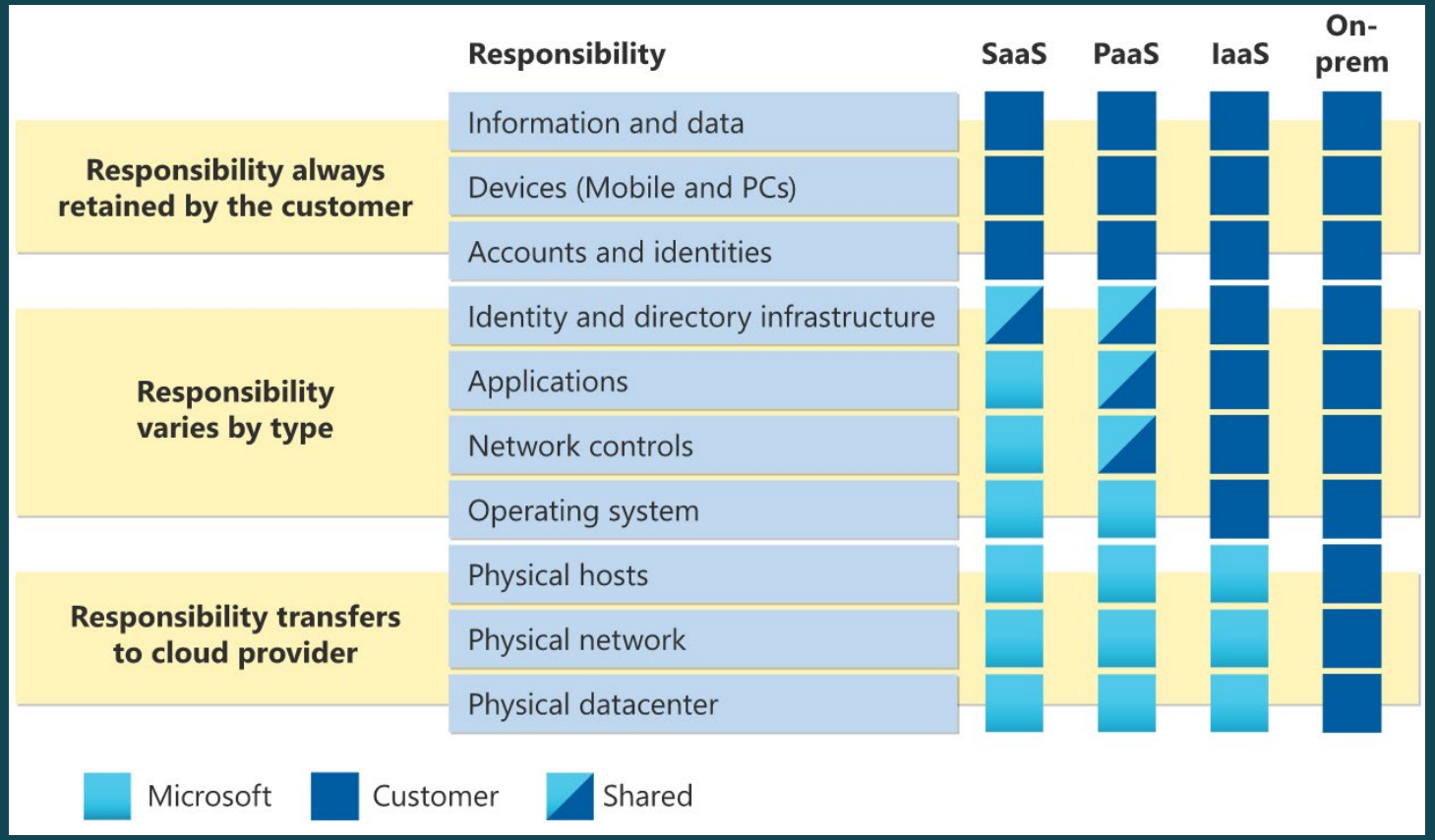
Cloud

Top cloud security threats

- **Misconfiguration and inadequate change control**
  - The complexity of cloud-based resources makes them difficult to configure.
  - Don't expect traditional controls and change management approaches to be effective in the cloud.
  - Use automation and technologies that scan continuously for misconfigured resources.
- **Insufficient identity, credential, access and key management**
  - Secure accounts, including the use of two-factor authentication.
  - Use strict identity and access controls for cloud users and identies--in particular, limit the use of root accounts.
  - Segregate and segment accounts, virtual private clouds and identity groups based on business needs and the principle of least privilege.
  - Take a programmatic, centralized approach to key rotation.
  - Remove unused credentials and access privileges.
- **Insecure interfaces and API**
  - Employ good API practices such as oversight of items like inventory, testing, auditing and abnormal activity protections.
  - Protect API keys and avoid reuse.
  - Consider an open API framework such as the Open Cloud Computing Interface (OCCI) or Cloud Infrastructure Management Interface (CIMI).
- **Account hijacking**
  - Don't just do a password reset when account credentials are stolen. Address the root causes.
  - A defense-in-depth approach and strong IAM controls are the best defense.
- **Limited cloud usage visibility**
  - Develop a cloud visibility effort from the top down that ties into people, processes, and technology.
  - Conduct mandatory company-wide training on accepted cloud usage policies and enforcement.
  - Have the cloud security architect or third-party risk management personnel eview all non-approved cloud services.
  - Invest in a cloud access security broker (CASB) or software-defined gateways (SDG) to analyze outbound activities.
  - Invest in a web application firewall to analyze inbound connections.
  - Implement a zero-trust model across the organization.

Cloud

Cloud hyper-scaler platforms have enabled many businesses to continue operations by simplifying user access to corporate information.

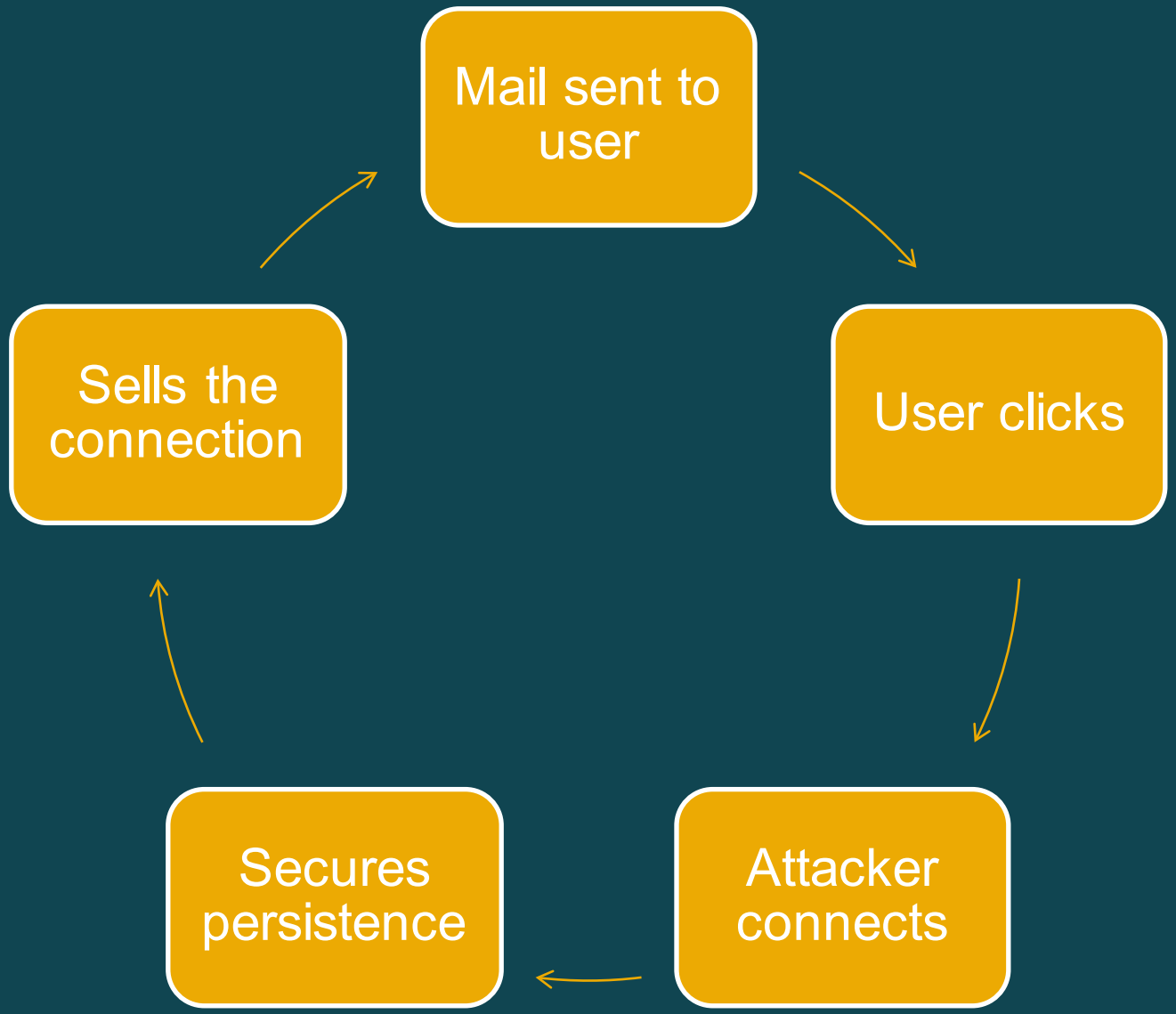


Other types of attacks on the Insurance Industry

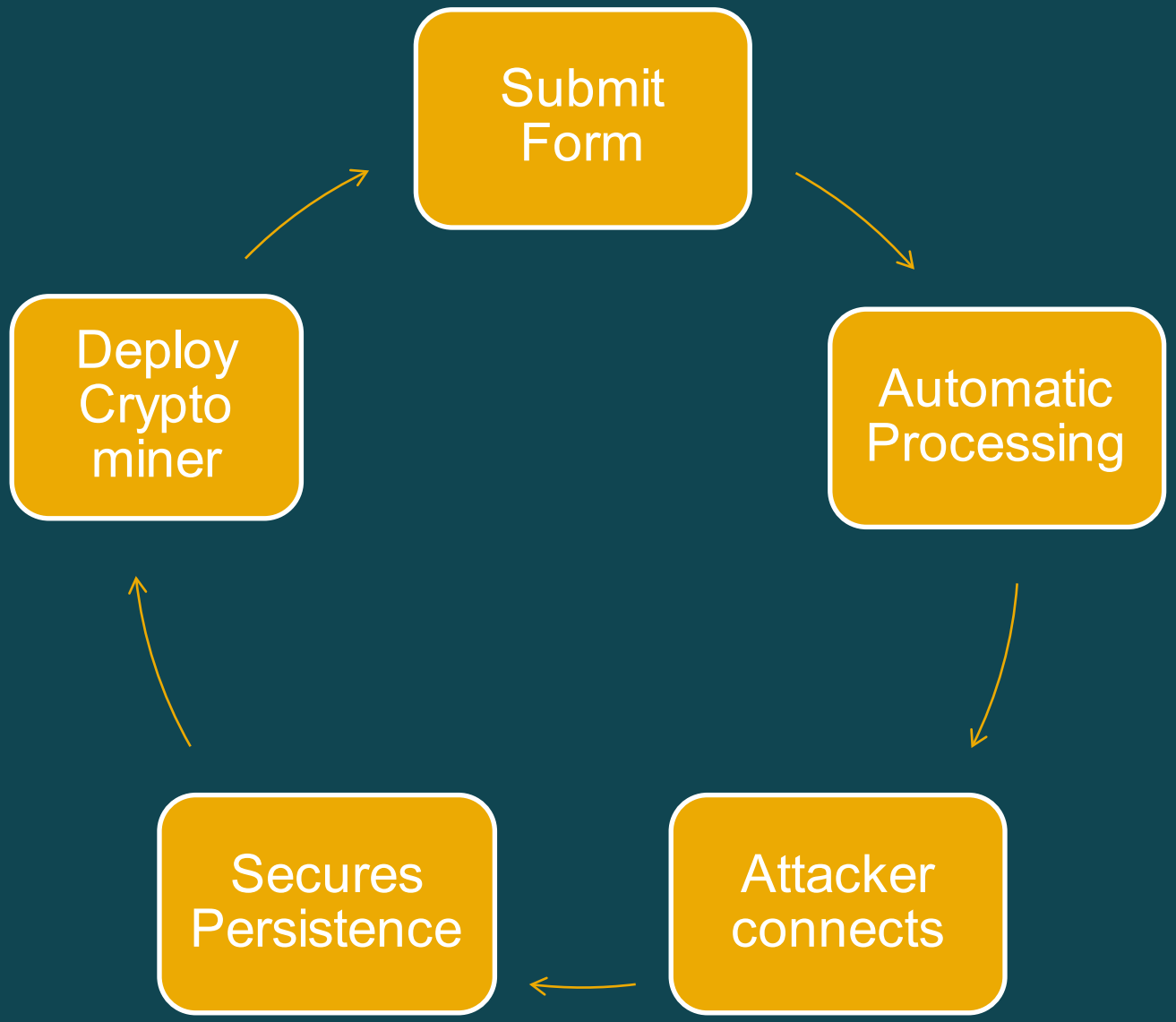
In addition to cloud born threats, insurance businesses face

1. ***Phishing***
2. ***File processing attacks***
3. ***Third party attacks***
4. ***Distributed denial of service***
5. ***Coin mining malware***
6. ***Ransomware***

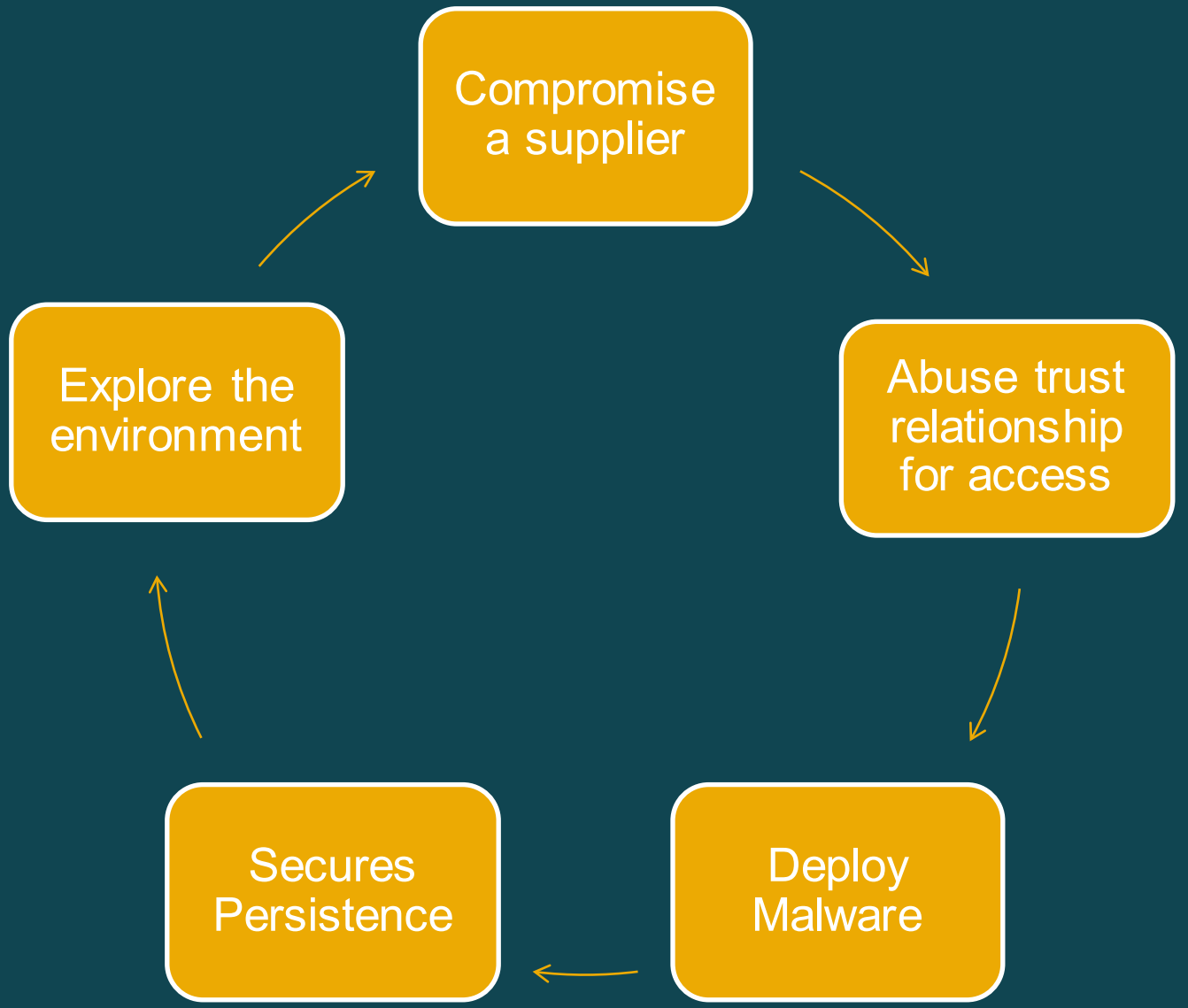
Attack Type 1: Attachment Phishing



Attack Type 2: File processing



Attack Type 3: Third Party



So how do we prepare

- Risk assessments and visibility
- Good policy
- Mature processes
- Implementation of a zero trust framework

Why Identity Centric Zero Trust (ICZT)

It only takes one compromised credential to potentially impact millions. Undeniably, identities and the trust we place in them, are being used against us.

Securing only endpoints, firewalls, and networks provides little protection against identity and credential-based threats. Until organizations start implementing identity-centric security measures, account compromise attacks will continue to provide a perfect camouflage for data breaches.

The ideology of ICZT

- never trust
- always verify
- enforce least privilege
- Assume a breach

Identity Defined Security

The Identity Defined Security Technology Components are like those used in many discussions around digital transformation, hybrid access, Zero Trust, etc.

Identity	Device	Network	Application	Infrastructure	Data
• Managing user lifecycles • Single Sign-on • Credential theft • Security Awareness training • Phishing Attacks • Service accounts • Privileged credentials • Third Party Risk	• Corporate managed vs unmanaged devices • Device risk and compliance posture state • Least privilege access • Encryption • Threat detection and response • Context driven device access	• The user is no longer on our network • Micro segmentation – VPN – Move towards ZTNA • Moving the traditional controls closer to the user (SASE) • DDOS attacks are a real threat	• On premises vs Cloud • Shadow IT • Access to Applications (Access Governance) • Access reviews • Secure Development of Applications • Securing deployed applications (WAF, BOT, DDOS)	• Vulnerabilities • Privileged access • Known and unknown infrastructure • Cloud and Hybrid environments • Security Posture in the cloud (CSPM) • Containerization	• Structured vs Unstructured Data • Data classification • Access to data (DAG) • Data Loss (accidental and malicious) • Visibility on data movement • Data protection • Data privacy (POPIA) • Ransomware