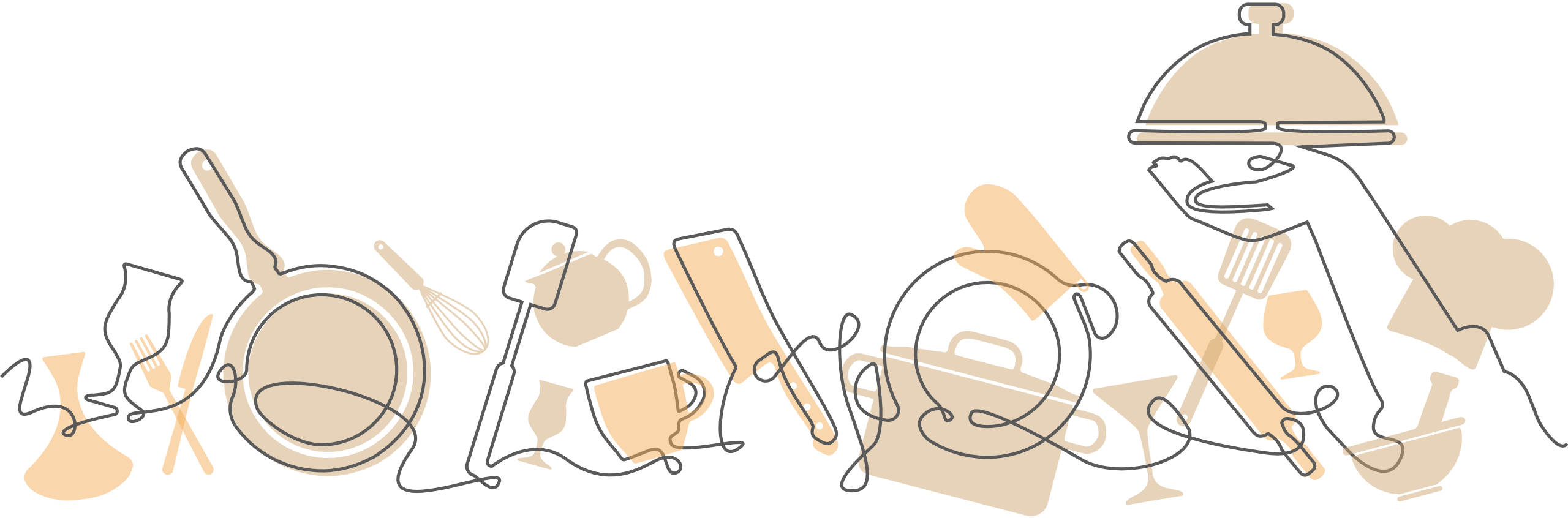


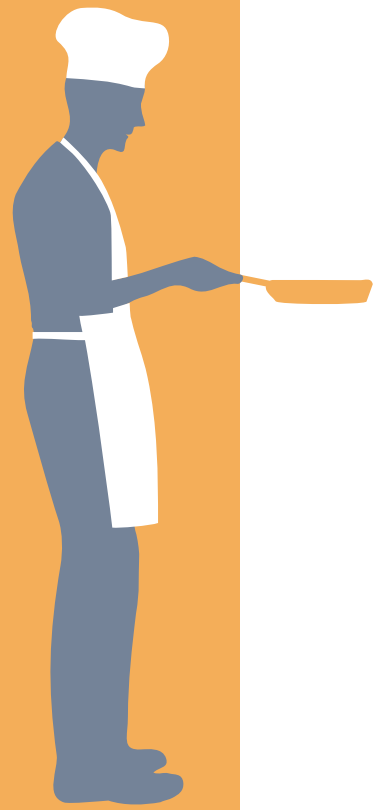
The CIO's Cookbook

Cybersecurity

Leading Thoughts

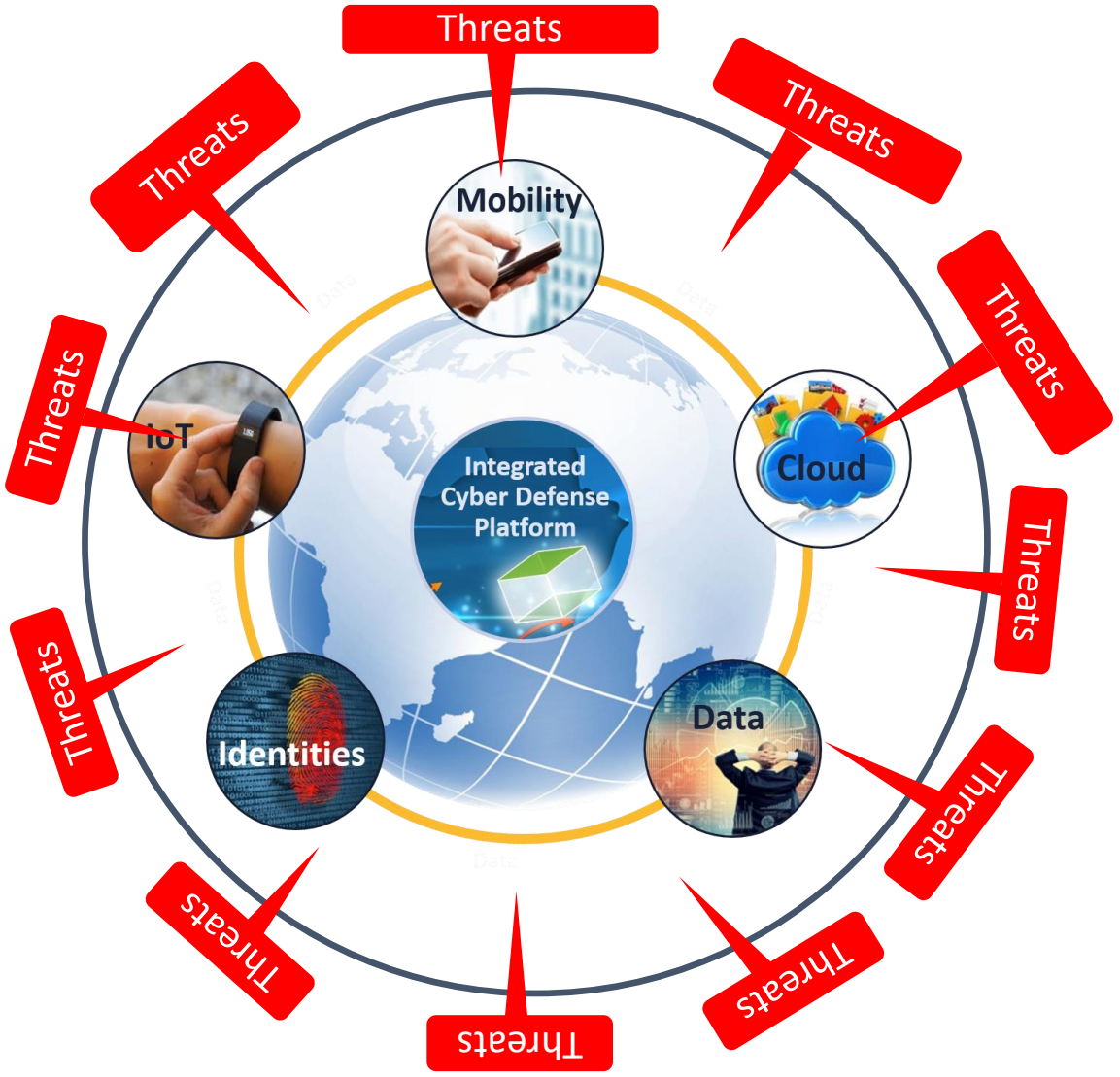
1. Expanding technology landscape from Digital Transformation has created more avenues for Threat Actors
2. Cybersecurity posture needs periodic assessment at the board level. Associated budgets cannot be an afterthought
3. Information Security is everyone’s business and not limited to just the CISO organization. Internal threats far exceed external threat vectors
4. Security Solutions and Suppliers are far too many. Does your organization have a “Cybersecurity” Architecture blueprint?

Considerations



1. CISO and CDO/CIO (Digital/Information) must perform complimentarily
2. Build a Culture to educate the workforce for securing the cyber and manage internal threats
3. Conform your technology practice with ISO Security standard
4. Assess security posture of your incumbent to be introduced public cloud providers
5. On-premise infrastructure & data can often get neglected. Build a predictable patching process
6. Build security for everything: EPM, Data, Identities & Access, Code, Infrastructure, Mail, & Network
7. Act not just to Identify & Protect. Build abilities to Detect, Respond & Recover from attacks
8. Implementing redundant solutions does not necessarily offer double protection.
   Build a Security Operations Centre just like your NOC

Threats are Increasing!



Digital security threats came from new and unexpected sources with sheer volume increasing. The threat landscape has become more diverse, with attackers working harder to discover new avenues of attack:

- **Malware—92% increase in download variants**
- **Email—55% spam rate**
- **Ransomware—46% increase in new attack variants**
- **IoT—600% increase in attacks**
- **Mobile—54% increase in attack variants**

Quite a challenge, but also an opportunity — building an integrated cyber defense platform

Cybersecurity Ecosystem

Secure DMZ
Email Gateway Security
Perimeter IDS/IPS
O365 AD Security
SWGs

Firewalls & VPN
Network Segmentation
Network Access Control
Encryption
Anti-spam
Network IDS/IPS
NAC

Endpoint Security
Patching & Configuration Management
Mobile Device strategy & Governance
Mobile Device Policy Management & MDM
BYOD Policy
Desktop Firewall
Anti-virus
DLP

Secure Code Reviews
Static/Dynamic App testing
App Vulnerability scanning
Encryption
WAF
Database Monitoring & Scanning

CASB
Cloud Workload & Data Security
Cloud Visibility & Assessment

PKI
Identity & Access management
Fulfilment (Account Provisioning)
End user Authentication
Privilege Access Management
Governance
Data Classification
Data Integrity Monitoring
Data-at-rest encryption

Policy Management
Threat & Vulnerability Management
Base Operational Metrics/Security Dashboard
SOC Monitoring
Incident Reporting, Detection & Response (CIRT)
Compliance Management – PCI, GDPR,FTC, FEdRAMP
Education, Training and Awareness

Managing Threats – Internal and External

Internal Threats

Lost or
Stolen Devices

Malicious
Insider

Employee
Mistakes

Other (policy avoidance, contractor misuse, lost storage devices)

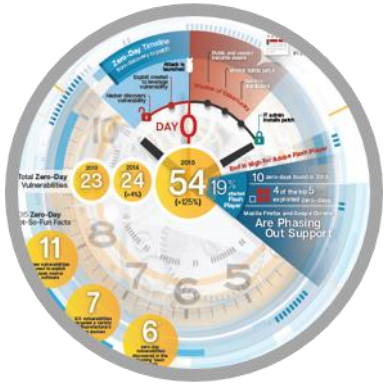
External Threats

Phishing

Advanced Malware
& Ransomware

Advanced Persistent
Threat or Advanced Actors

Stolen or lost
credentials



Zero Days and
Vulnerabilities