Cyber Risk – New Solutions

Agenda

01 Setting the Context

02 Dirty Seven & Modus Operandi

03 Lessons Learnt & New Solutions

04 Q&A

Section 1

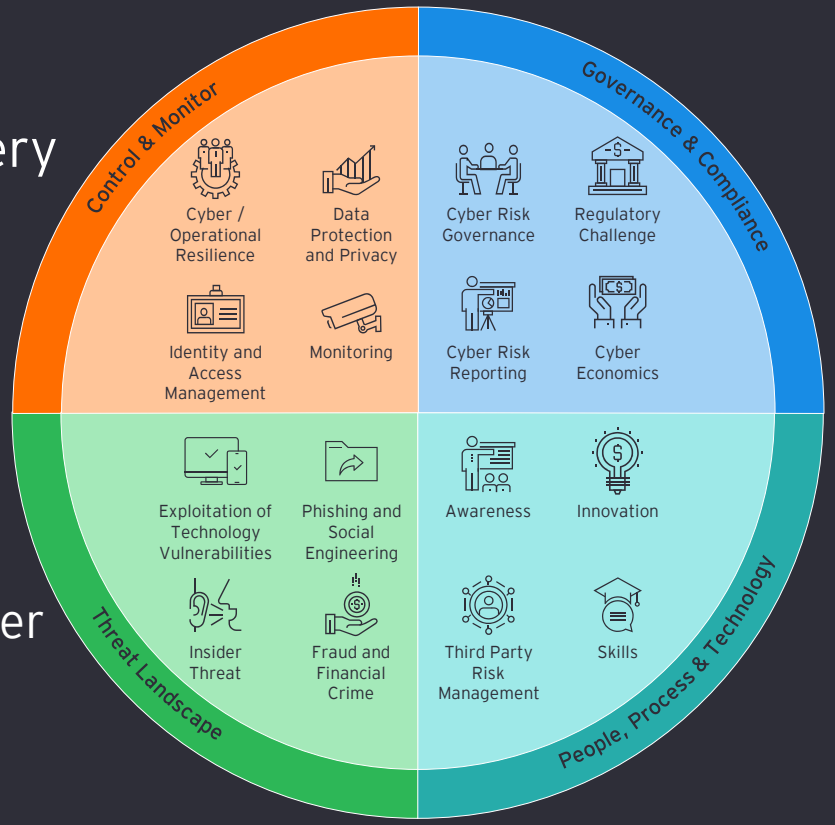
Setting the Context – Recent Incidents & Trends

Cyber Risk.. Hype or Reality?

Cyber Attack for every 1 second

Global Cost of Cyber Crime $4 trn+

Number of Malwares per day 8 million +



Average time to detect an attack -162 days

Average time to bring back critical operations to normalcy 4 days

AI/ML base Malwares - Sandbox aware Malwares

Cyber Security – Cost Centre or Business Enabler?

Current Scenario...

Some notable Cybersecurity statistics

Inadequate operating models

In 2021, **80%** of firms have seen an increase in Cyber attacks.

21% Financial and Manufacturing services have the highest percent of exposed sensitive files at 21%.

71%

71 percent of all data breaches were financially motivated and 28 percent of which involved insiders. [6]

86%

of organizations were compromised by a successful cyberattack in 2021. According to a recent report, more than three-quarters of IT security professionals believe a successful cyber attack is imminent in 2021. [5]

ISO, NIST, SOC and CCPA are some of the compliance and regulatory standards to streamline the process for technology adoption, provide clarity on the regulator's expectations and address any prevalent Cyber misconceptions.

What leadership thinks...

75% of CISOs are not confident that they can quantify, in financial terms, the effectiveness of their spending. [2]

84% of organizations say they are not getting adequate board level reporting for cyber risk. [4]

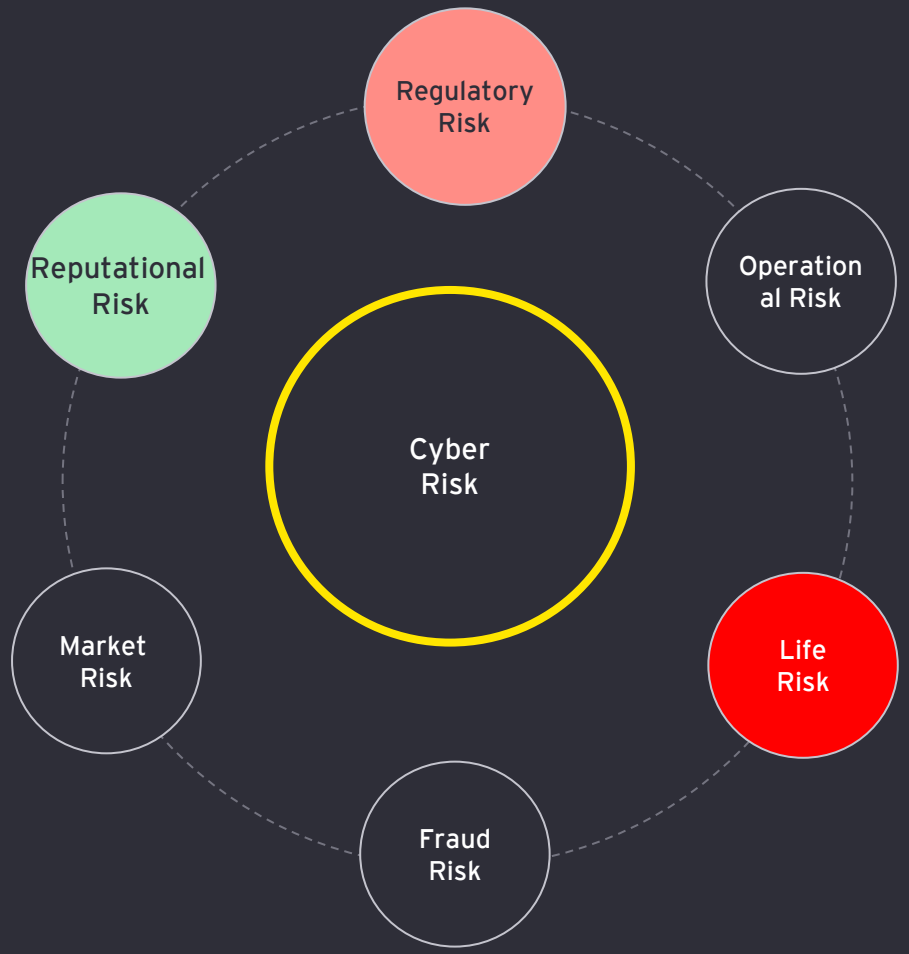
26% of companies say a lack of executive awareness of management/governance issues limits the value of their security function. [1]

80% of boards are not confident in their organizations cyber-attack mitigation measures. [3]

Percent of companies that say their cybersecurity function does NOT meet their needs. [1]

1. How utilities can sustain and enhance trust with their stakeholders
2. How next-generation CISOs can become agents of change
3. How will your business bridge the cybersecurity divide?
4. Cybersecurity: How firms can protect, optimize and enable
5. Cybersecurity attacks 2021
6. Data Risk Report Stats
7. 2020 Data Breach Investigations Report

Various Cyber Risks..



- Carbanak Attack – European banks
- Cosmos Bank
- Bangladesh Heist
- Cyber attacks on Colonial Pipeline

CDSL malware attack hits broking ops; Sebi, Cert-in to probe incident

Brokering industry players said the disruption caused by the malware attack could have been more adverse if not for the weekend

Cyber attack at AIIMS Delhi: Hackers demand Rs 200 cr in crypto, says report

The ransomware attack is being looked into by the Delhi Police, the Ministry of Home Affairs, and the India Computer Emergency Response Team (CERT-IN).

TATA

14th October 2022
BJ/SH-L2N/

BSE Limited
Corporate Relationship Department
1st Floor, New Trading Ring,
Rotunda Bldg., P. J. Towers,
Dalal Street, Fort,
Mumbai 400 001.
Scrip Code: 500400

National Stock Exchange of India Limited
Exchange Plaza,
Bandra Kurla Complex
Bandra East
Mumbai – 400 051
Scrip Code: TATAPOWER EQ

Dear Sirs,

Cyber attack

The Tata Power Company Limited had a cyber attack on its IT infrastructure impacting some of its IT systems.

The Company has taken steps to retrieve and restore the systems. All critical operational systems are functioning; however, as a measure of abundant precaution, restricted access and preventive checks have been put in place for employee and customer facing portals and touch points.

The Company will update on the matter going forward.

Yours faithfully,
For The Tata Power Company Limited

HANOZ MINOO MISTRY
Digitally signed by HANOZ MINOO MISTRY
Date: 2022.10.14 18:56:57 +05'30'

H. M. Mistry
Company Secretary

Oil India suffers cyber attack, receives Rs 57 crore ransom demand

Hive Ransomware Group claims responsibility for Tata Power Data Breach

The Hive group, which is said to be barely a year old in the scene, targets energy, healthcare, financial, media, and education sectors.

SpiceJet ransomware attack: Hundreds of passengers stranded

Hundreds of Indian air travellers were stranded inside their planes after the low-cost airline SpiceJet cancelled or delayed flights due to an "attempted ransomware attack", the company has said.

Cyber Attacks on Critical Sector's - Nuclear, Power, Water supply, Telecom.....

Cyber-attack on Kudankulum Nuclear Power Plant underlines the need for cyber deterrent strategy

Israel appears to confirm it carried out cyberattack on Iran nuclear facility

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.

LightBasin hackers breach 13 telcos in two years

‘Cyberpartisans’ hack Belarusian railway to disrupt Russian buildup

Activists claim they could paralyse trains moving Russian forces for potential attack on Ukraine

A train carrying Russian military hardware at a railway station in Belarus. Photograph: Russian Defence Ministry/Tass

Russia is using an onslaught of cyber attacks to undermine Ukraine’s defence capabilities

Published: February 24, 2022 5.29am GMT

Getty Images

Email
Twitter 38
Facebook 119
LinkedIn

As Ukrainian cities come under air attack from Russian forces, the country has also suffered the latest blows in an ongoing campaign of cyber attacks. Several of Ukraine’s bank and government department websites crashed on Wednesday, the BBC reports.

72 Groups.. Pro Ukraine/Russia

GROUP	SUPPORTS	TYPE	COMMS	LOC
Anonymous Associated				
BlackHawks	Ukraine	DDoS/Hack	Twitter	Georgia
LiteMods	Ukraine	Psyops/DDoS	Twitter	UNK
SHDWSec	Ukraine	Hackivism	Twitter	UNK
N3UR0515	Ukraine	DDoS	Twitter	UNK
PuckArks	Ukraine	Pysops	Twitter	UNK
GrenXPaRTa_9haan	Ukraine	Databreach	Twitter	Indonesia
YourAnonNews	Ukraine	Psyops	Twitter	UNK
DeepNetAnon	Ukraine	Radio/hack	Twitter	UNK
Anonymous Younes	Ukraine	DDoS/Hack	Twitter	UNK
0xAnonLeet	Ukraine	DDoS/hack	Twitter	UNK
AnonGh0st	Ukraine	DDoS/Hack	Twitter	UNK
Anonymous Romania	Ukraine	DDoS/Hack	Twitter	Romania
Shadow_Xor	Ukraine	Databreach	Twitter	UNK
PuckArks	Ukraine	Defacement	Twitter	UNK
Squad303	Ukraine	DDoS/SMS	Twitter	Poland
Synthynt	Ukraine	Ransomware	Twitter	UNK
GhostSec	Ukraine	Hack	Telegram	UNK
DDoS Secrets	Ukraine	Databreach	Twitter	UNK
v0g3lSec	Ukraine	Hack	Twitter	UNK
Anonymous News	Ukraine	DDoS	Twitter	UNK
DoomSec	Ukraine	DDoS/Hack	Twitter	UNK
CyberNinja Security Team	Ukraine	Hack	Twitter	UNK
ReaperSec NEW	Ukraine	Hack/DDoS	Twitter	UNK
HAL9000 NEW	Ukraine	Hack/DDoS	Twitter	UNK
RedCult NEW	Ukraine	Hack/DDoS	Twitter	UNK
Nation-State				
GhostWriter UNC1151	Russia	Hack	UNK	Belarus
SandWorm	Russia	Hack	UNK	Russia
Gamaredon	Russia	Hack	UNK	Russia
DEV-0586 APT	Russia	Hack	UNK	Russia
DEV-0665 APT	Russia	Hack	UNK	Russia
FancyBear APT	Russia	Hack	UNK	Russia
IT Army of Ukraine	Ukraine	DDoS	Twitter	Ukraine
IT Army of Ukraine Pysops	Ukraine	Pysops	Twitter	Ukraine
Internet Forces of Ukraine	Ukraine	Pysops	UNK	Ukraine
MustangPanda APT	UNK	Hack	UNK	China
Curious George	UNK	Hack	UNK	China

GROUP	SUPPORT	TYPE	COMMS	LOC
Pro-Ukraine Groups				
BlueHornetAPT49 (ATW)	Ukraine	Hack	Twitter	UNK
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK
GNG	Ukraine	DDoS	Twitter	Georgia
Spot	Ukraine	DDoS	Twitter	UNK
GhostClan	Ukraine	DDoS/Hack	Telegram	UNK
1LevelCrew	Ukraine	DDoS	Twitter	UNK
Hydra UG	Ukraine	Radio	Twitter	UNK
SecJuice	Ukraine	OSINT/Psyop	Twitter	UNK
Ring3API	Ukraine	Hack	Twitter	Ukraine
Belarusian Cyber-Partisans	Ukraine	Ransomware	Twitter	Belarus
NB65	Ukraine	Ransomware	Twitter	UNK
Monarch Turkish Hacktivists	Ukraine	Defacement	UNK	Turkey
Shadow_Xor	Ukraine	UNK	Twitter	UNK
The Connections	Ukraine	UNK	Twitter	UNK
Rabbit Two	Ukraine	Hack/DDoS	Twitter	UNK
SecDet	Ukraine	Hack	Twitter	US
BeeHive Cybersecurity	Ukraine	Phishing/hack	Twitter	UNK
Cyber_legion_hackers	Ukraine	Deface/DDoS	Twitter	UNK
Stand for Ukraine	Ukraine	hack/ DDoS	UNK	Ukraine
BrazenEagle (ATW)	Ukraine	Hack	Telegram	UNK
Bandera Hackers	Ukraine	Hack/DDoS	Twitter	UNK
HackenClub	Ukraine	DDoS/hack	Twitter	Ukraine
Pro-Russia Groups				
RedBanditsRU	Russia	Hack	Twitter	Russia
Stormous Ransomware	Russia	Ransomware	Telegram	UNK
Hydra	Russia	Dox/DDoS	Twitter	Russia
RaHDit	Russia	Hack	UNk	Russia
Xaknet	Russia	Hack	Site	Russia
Killnet	Russia	Hack/DDoS	Telegram	Russia
404 Cyber Defense	Russia	DDoS	Twitter	UNK
WeretheGoons	Russia	Hack	Twitter	Russia
punisher_346	Russia	PsyOps	Twitter	UNK
Lorec53	Russia	Hack	UNK	Russia
DDoS Hacktivist Team	Russia	DDoS	Telegram	Russia
cyberwar_world	Russia	Hack/ddos	Telegram	Russia
Zsecnet NEW	Russia	Hack/DDoS	Telegram	Russia
DivisionZ NEW	Russia	Hack/DDoS	Telegram	Russia

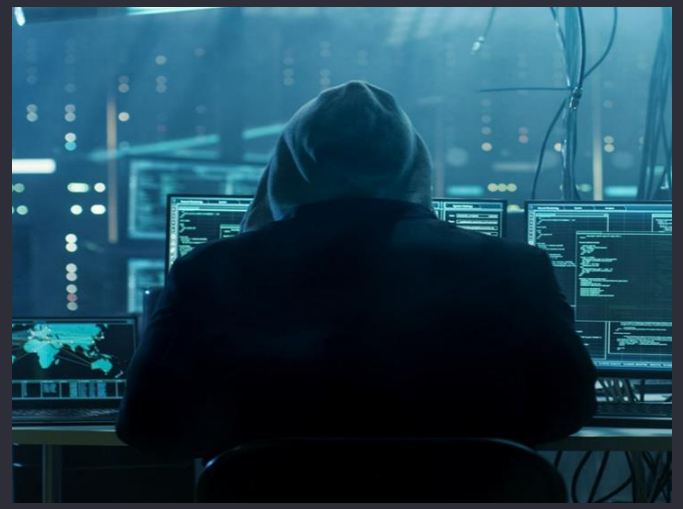
Hacktivism……DragonForce Malaysia (Telegram Group)

Malaysian Hacktivist group DragonForce issues a clarion call to other hackers to target India

Following the controversial remark by former BJP spokesperson Nupur Sharma on Prophet Muhammad, a Malaysian Hacking Group has initiated a hacking campaign against India - #OpsPatuk

Current Trends

- ✓ Gap between Digital Technologies and Cyber Security Products
- ✓ Targeted Attacks – Specific to Sector, Have SME's
- ✓ Software Vulnerabilities to Hardware Vulnerabilities
- ✓ Increase in Attack Surface – API's/ Cloud
- ✓ Threat Actors.. APT attacks
- ✓ Attacks are getting more modular- " My Part … Your Part"..
  - Initial Access Brokers
- ✓ Exchange of tools between "Threat Actors"
- ✓ Own exploit Kits & Framework – R&D, not for commercial sale.
- ✓ Anti- Forensics Techniques used by the attackers

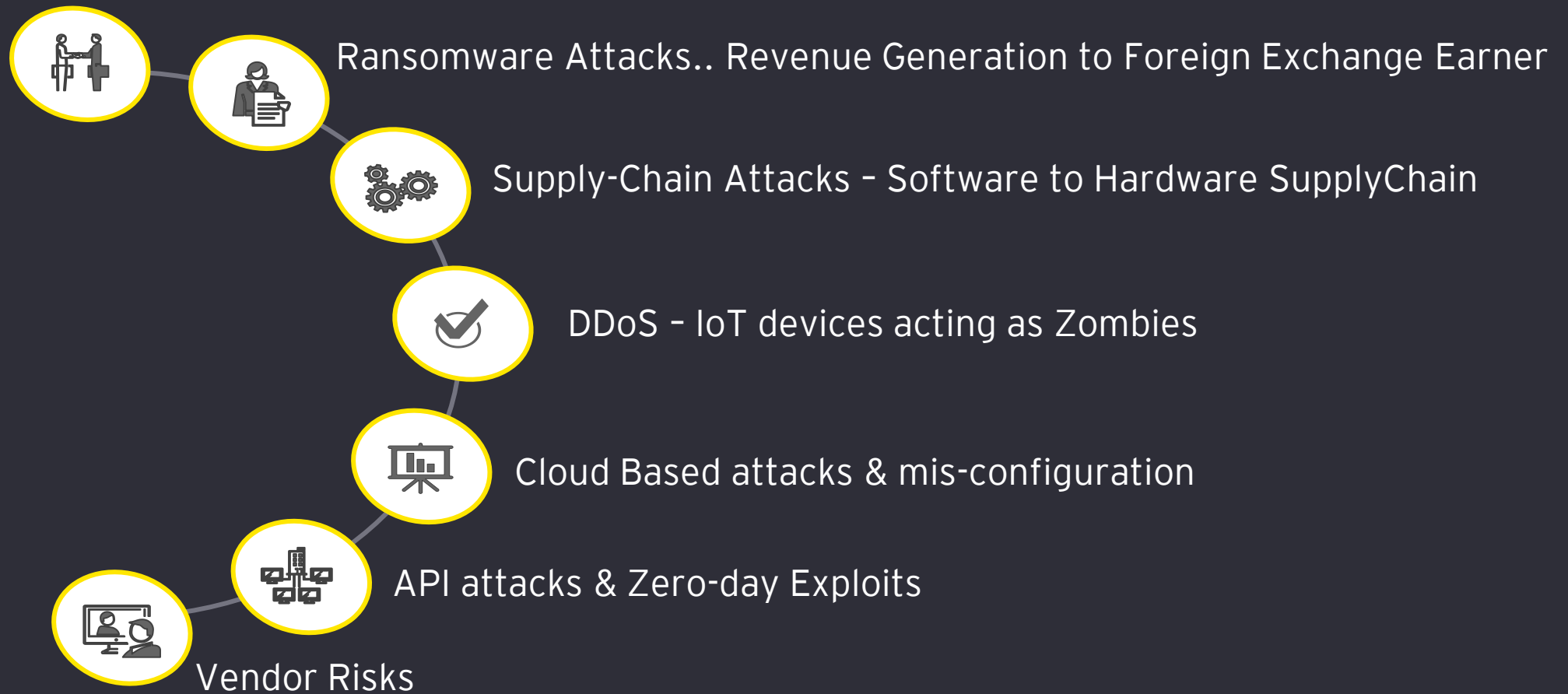


Section 2

Dirty Seven & Modus Operandi

The Dirty Seven..

Social Engineering attacks - Phishing, Smishing, Vishing, QRishing (QR Code Phishing)



Ransomware Attacks.. Revenue Generation to Foreign Exchange Earner

Supply-Chain Attacks – Software to Hardware SupplyChain

DDoS – IoT devices acting as Zombies

Cloud Based attacks & mis-configuration

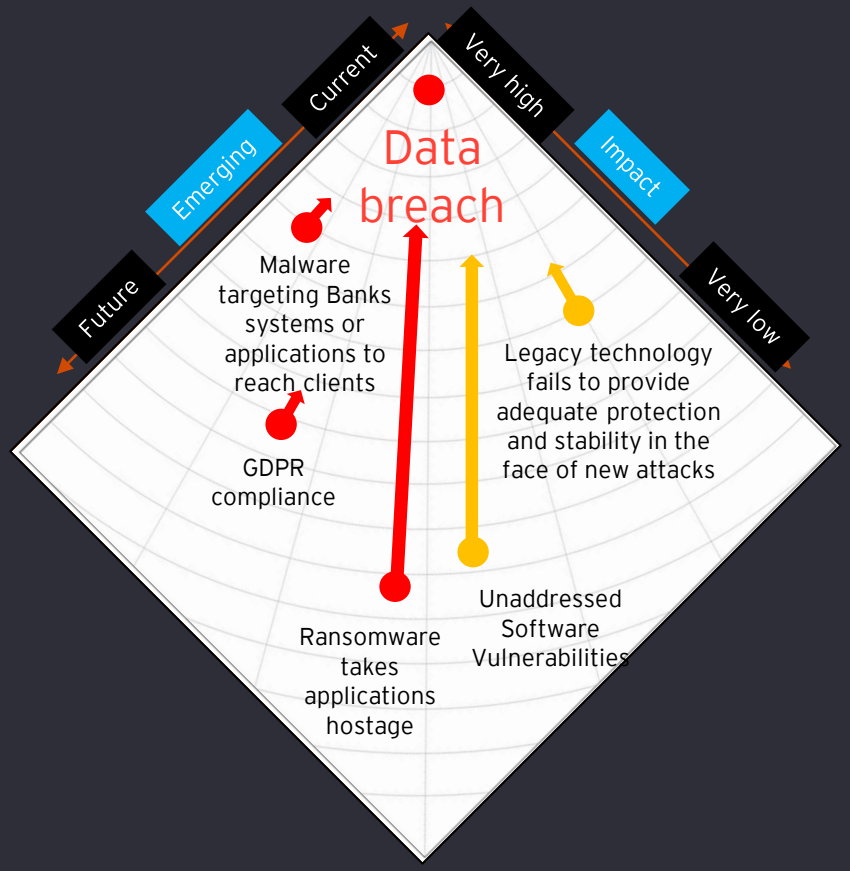
API attacks & Zero-day Exploits

Vendor Risks

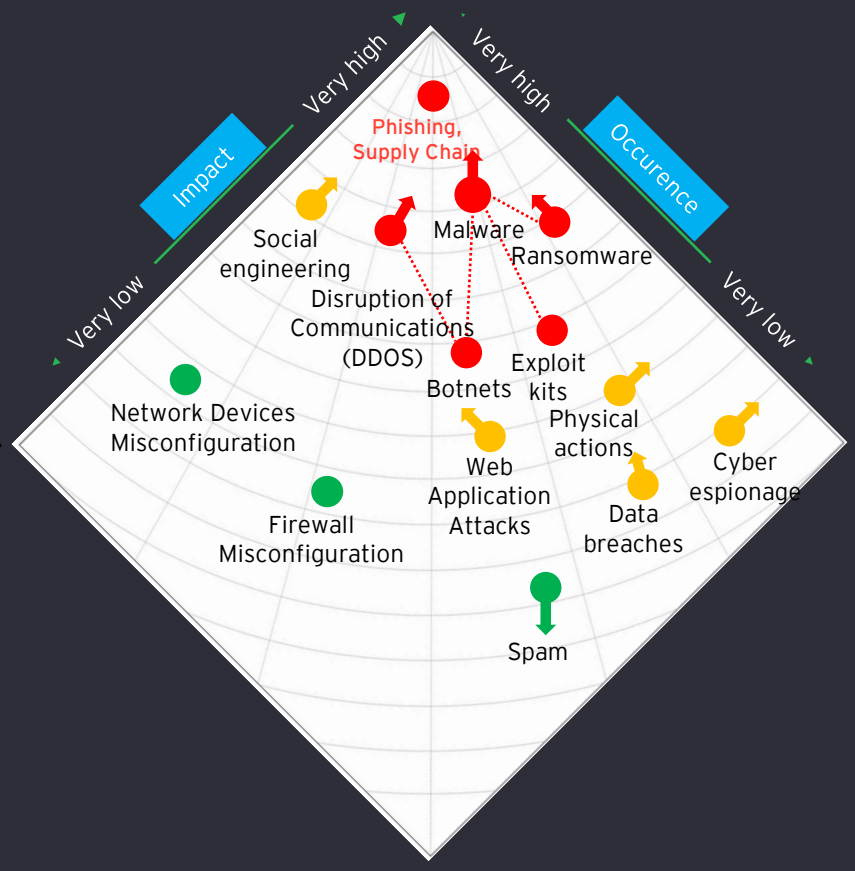
Threat Scenario

HIGH MED LOW

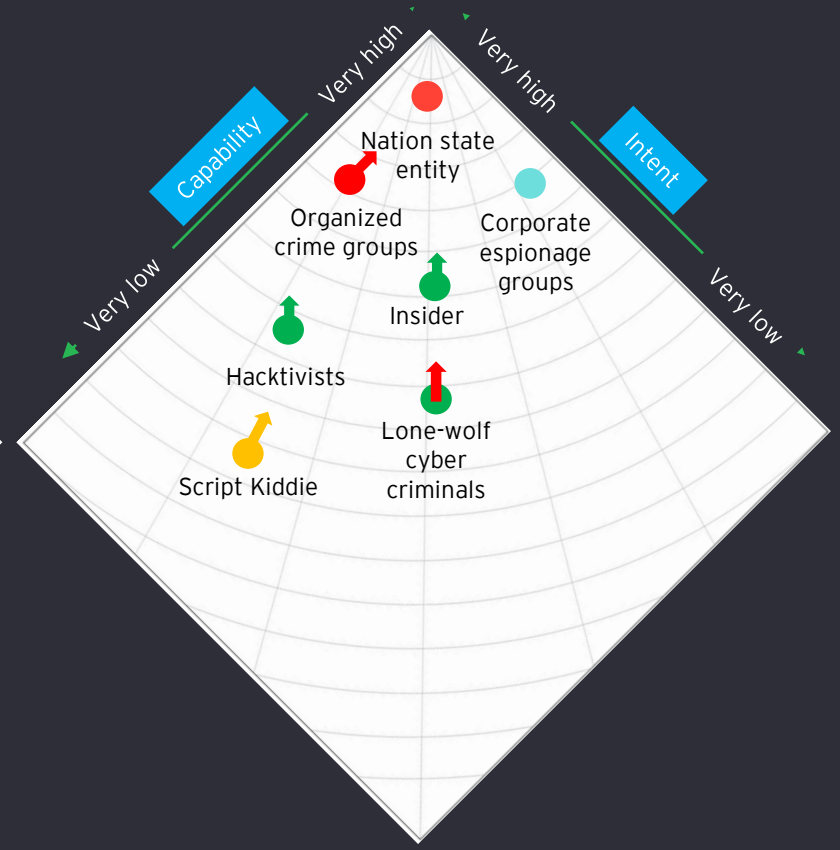
TOP THREAT SCENARIOS



TOP ATTACK VECTORS

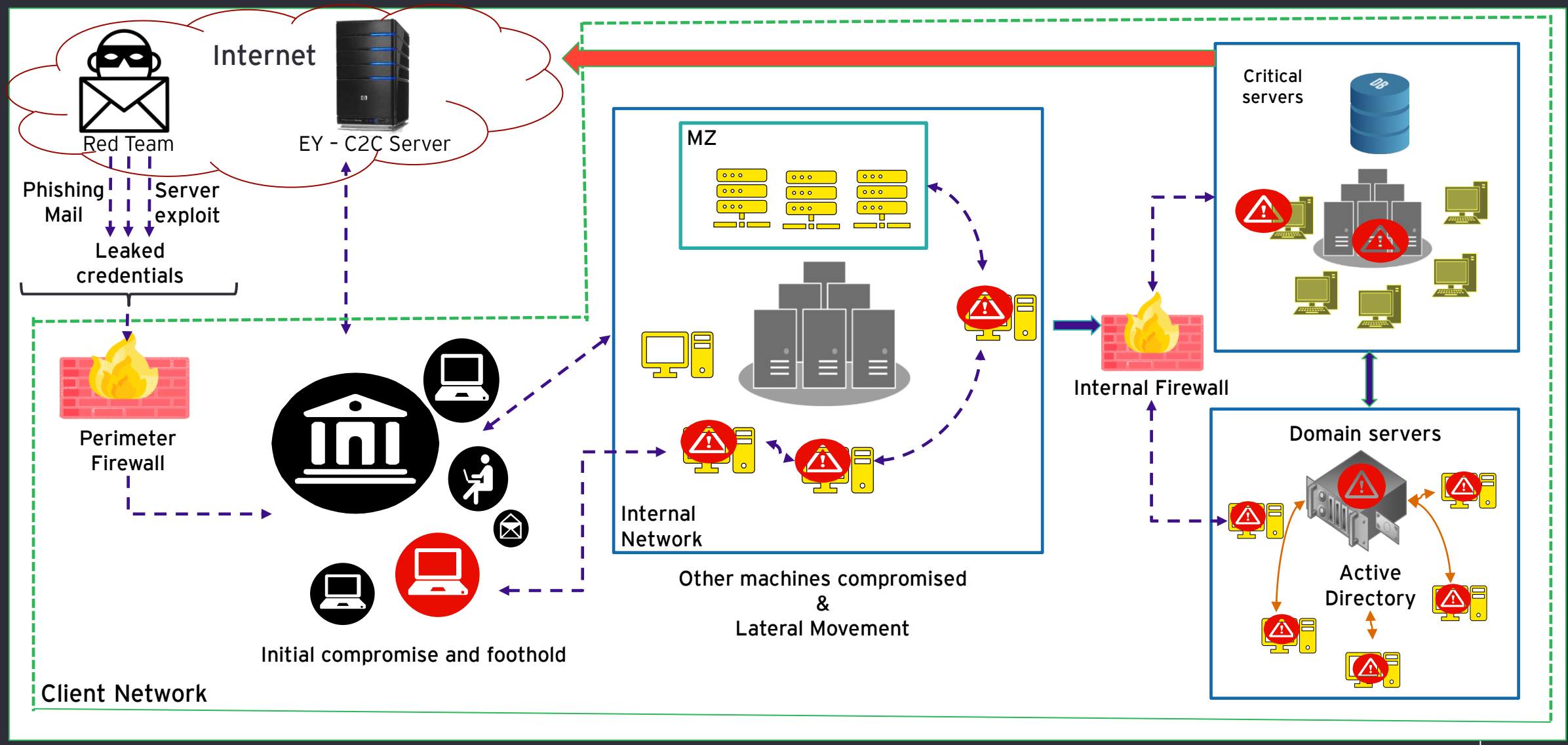


TOP ADVERSARY GROUPS



Sources: Threat Intelligence & Analysis program

Modus Operandi of attacks



Section 3

Lessons Learnt & New Solutions

What has been done so far…

Cyber Security - **Policy, Framework, Governance**

Cyber Security Awareness to all employees – **Do's & Don'ts**

Intranet & Internet Separation – **DMZ & MZ**

Blocking USB, Encrypting data at Rest/Transit - **Data Leakage and Data Security**

Identify Your **"Crown Jewels" – Data Governance/ Owner/Custodian**

SIEM & Security Operation Centre– "**monitoring the activities in real-time, user behaviour analytics**"

Technology solutions – **AV, Firewall, IDS, IPS, WAF, DAM, IDAM / PIM** etc.,

Lessons Learnt?

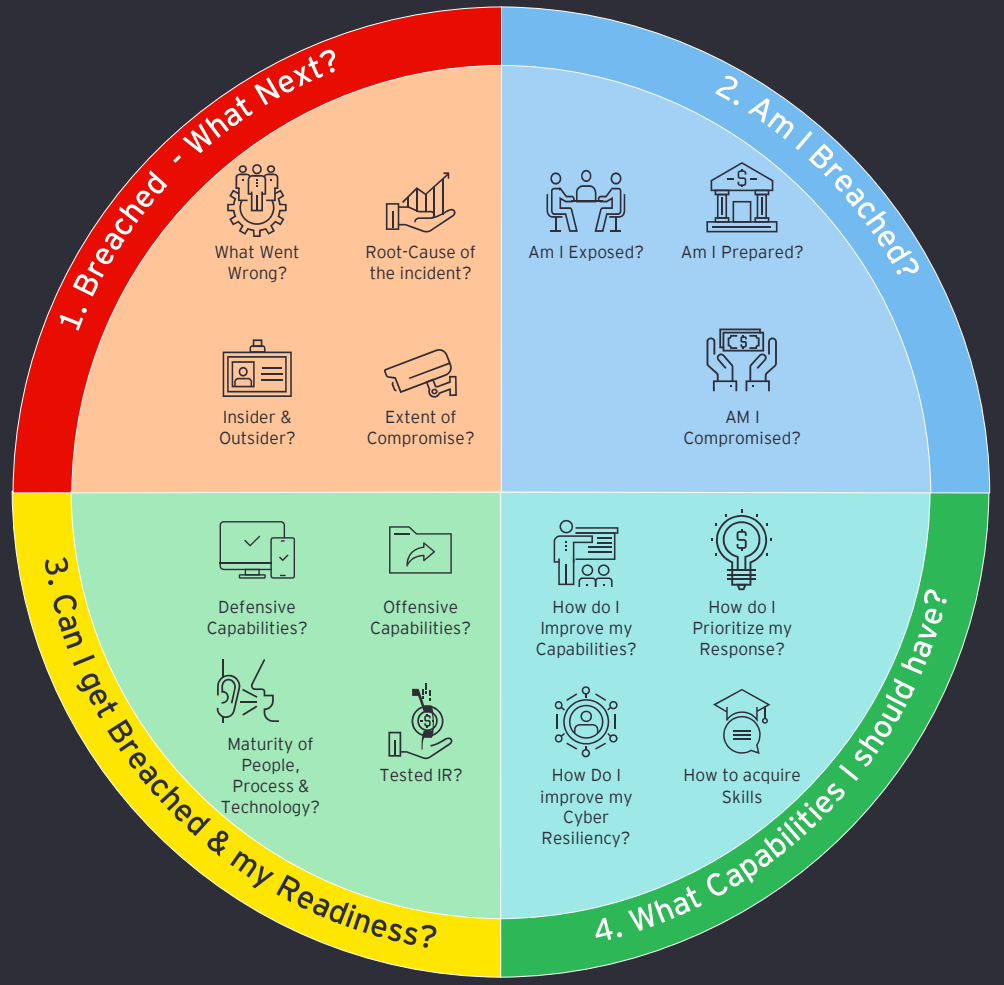
100% Cyber Security Myth

Protect, Detect, Respond to Detect, Respond, Protect

Lessons Learnt

Eradication not possible.. Only Mitigation

Reactive to Proactive to Predictive - AI/ML



Weakest Link... Cyber Hygiene

96% of data breaches can be attributed to human error

'PEOPLE' are not the WEAKEST LINK, they are in fact the 'PRIMARY ATTACK VECTOR'

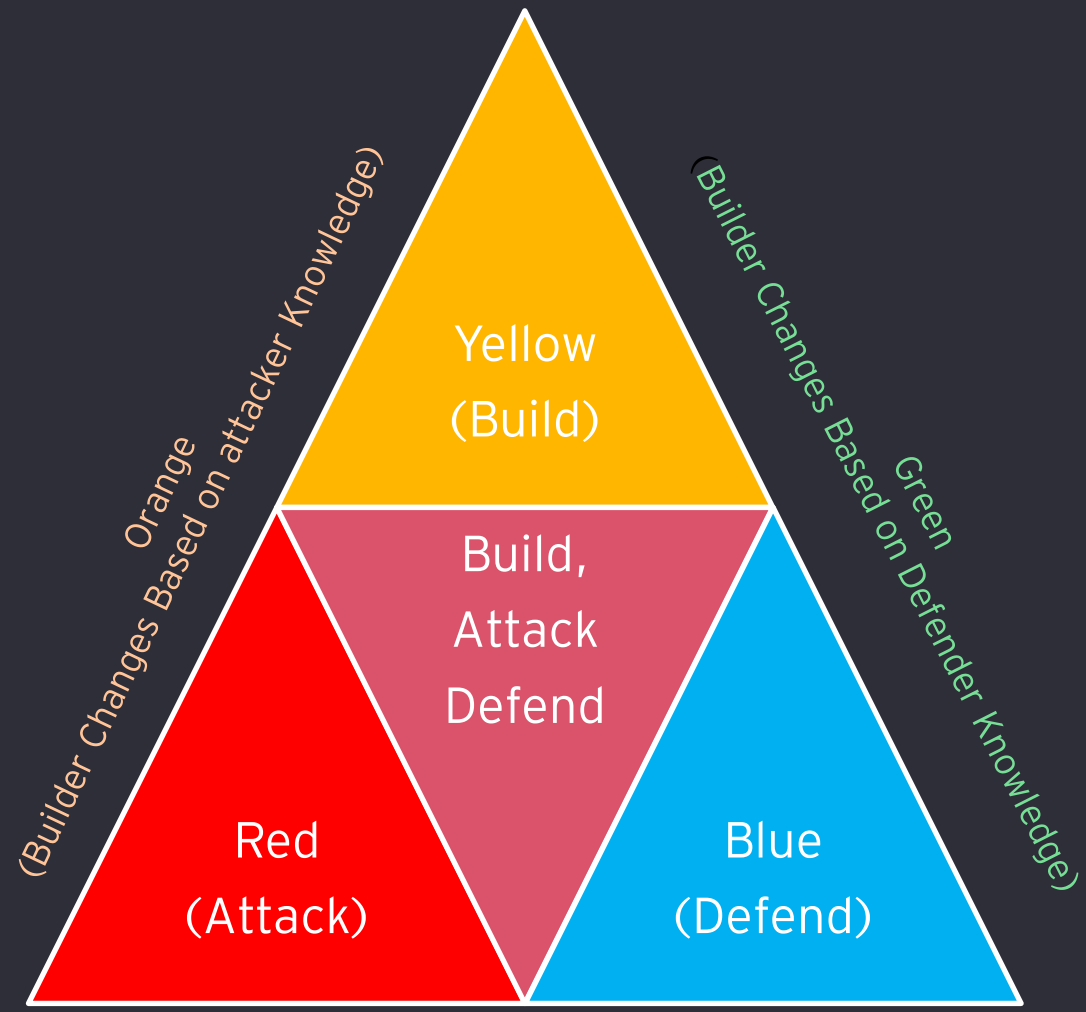
Who are going to be our 'weakest link' or 'greatest strength'

Change of Strategy

01 Absolute Risk not Relative Risk

02 Defensive to Offensive Capabilities

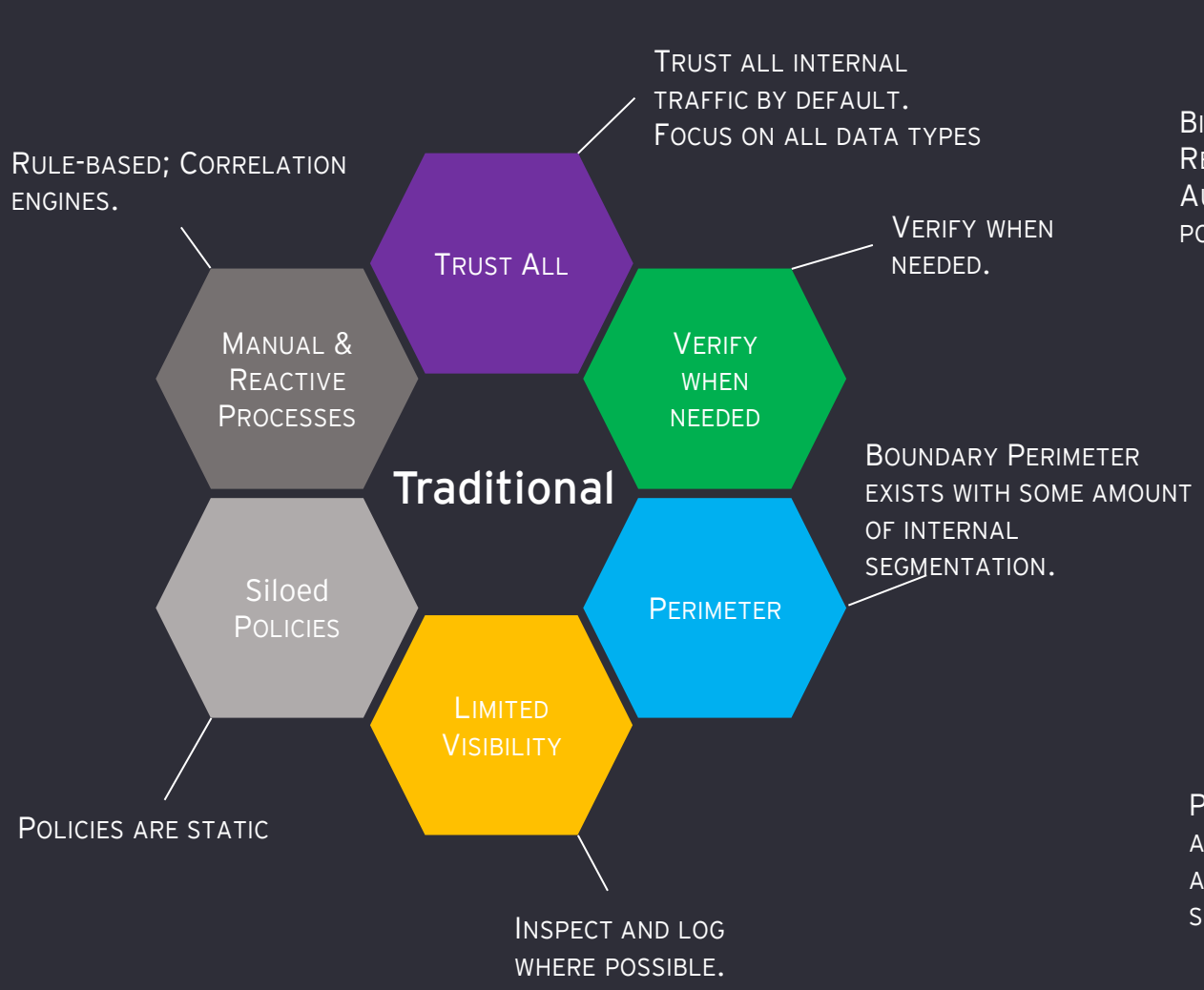
03 Early Detection and Rapid Response

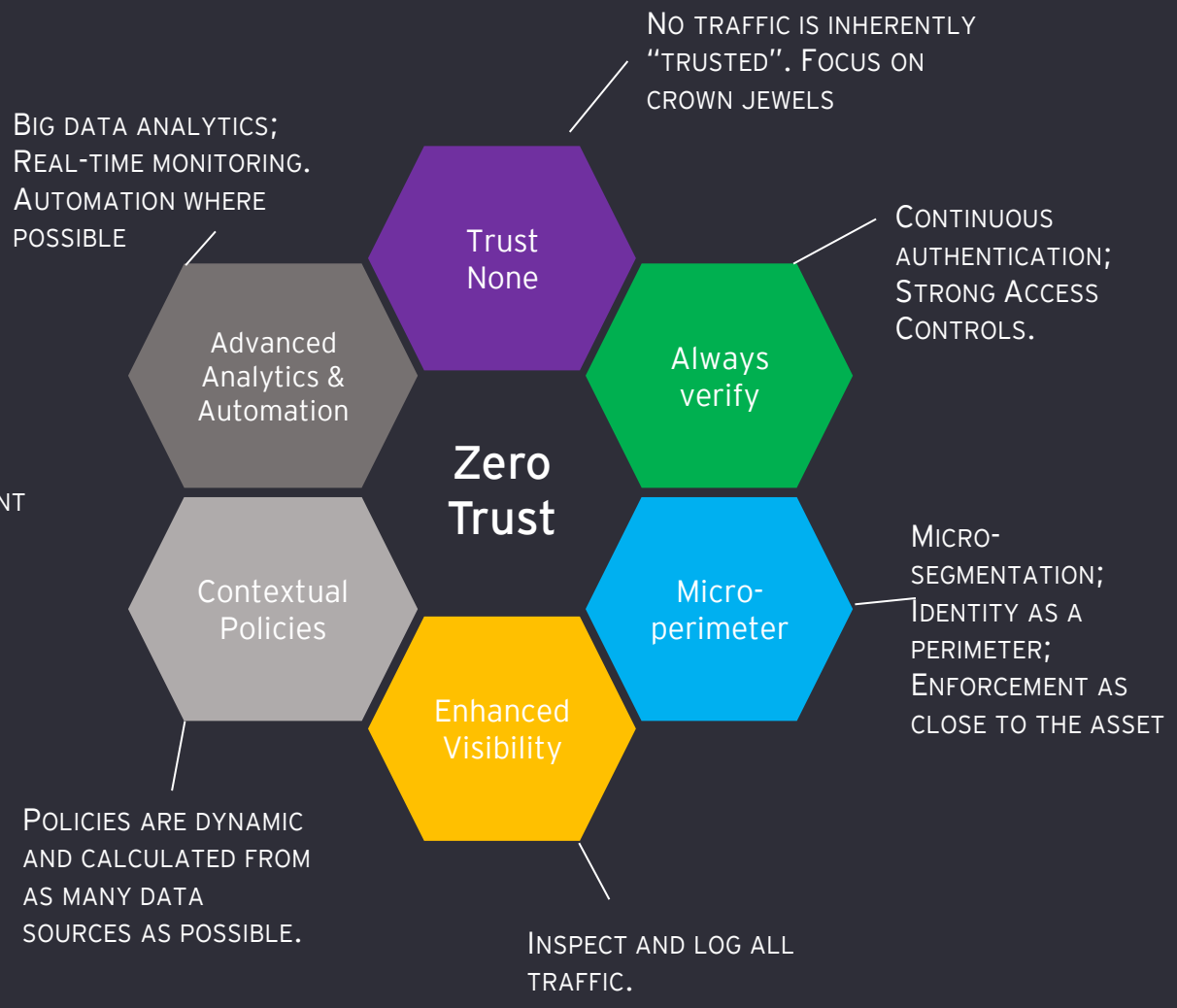


Trust is a vulnerability.

John Kindervag
Field CTO, Palo Alto Networks

Traditional Architecture to Zero Trust Architecture





WORKLOAD
(Devices, Data, Applications)

WORKPLACE
(Cloud, On-Prem, Remote, Network)

WORKFORCE
(Staff, Contractors, Vendors)

Cognitive and Convergent Cybersecurity Platform

Linked Data from external sources

- TI FEEDs
- OSINT
- Intel from Social Media
- VA SCANs
- Market Feeds
- Fraud
- Attack Surface analysis

Data sources from within the organization

- Logs (Applications & Endpoints)
- Cloud
- Packets
- NetFlows
- Asset Discovery

- Big Data
- AI & ML
- BOTs
- SOAR

Analysis & Desired outcomes

- Compliance to RBI, SOX, PCI-DSS, GDPR, DPAs
- Vulnerabilities/Exploits using VDB | MITRE ATT&CK Framework or/and Vulnerability databases
- Compliance to 27K1/NIST 800-53
- And more....

The NextGen platform

- A Big Data platform with built-in machine learning driven advanced behavioural analytics, threat hunting capabilities
- Built-In Automation for Incident & Forensics Life Cycle Management to Protect, Detect, Respond, Remediate & Investigate evolving threats

Enterprise Cyber Supply Chain Risk Management

Software Supply Chain Security helps organizations detect, identify, analyse, and mitigate risks associated with the components required for software development

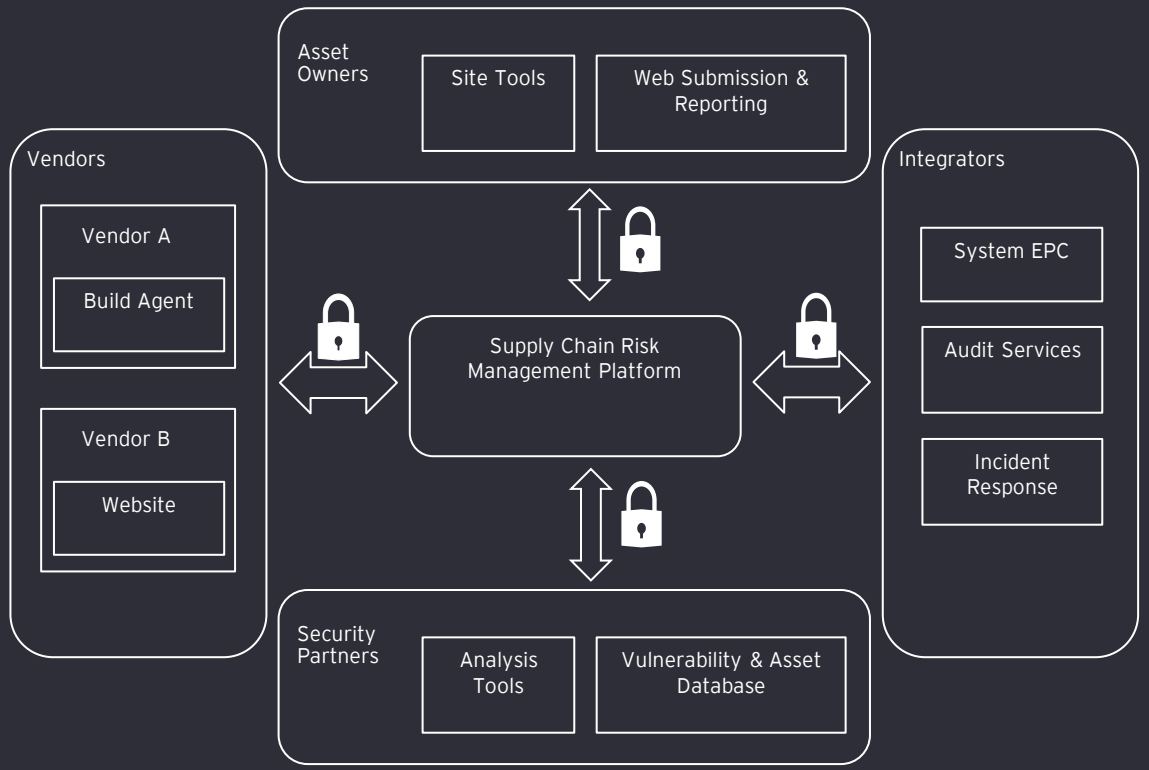
What is Software Supply Chain Security?

Software Supply Chain Security refers to securing the different components for developing a software and maintain security best practices in the activities involved in the development or deployment process.

Securing the software supply chain requires following few security practices:

- Assess the security and trustworthiness of the third-party code.
- Ensure that the proprietary code is secured.
- Secure the data transfer method used by applications.
- Continuously test and monitor the code after deployment to identify any threat.
- Provide consumers with Software Bill of Materials (SBOM).

Supply Chain Risk Management Conceptual Model



Assess the Supply Chain

Assess the application's dependencies to know what is involved in each step of the SDLC, who are the contractors,and how the software updates are installed. There should be an audit conducted for all the access rights granted to internal and external parties for the applications.

Access Management

Closely monitor the privileged accounts for unusual activities. Respond to the unwanted password change, login activity, and permission changes.

Fix Vulnerabilities

IT Team must perform a software composition analysis to find unknown vulnerabilities in third-party and fix with patches.

Other Tech solutions

Attack Surface Management

DevSecOps – Secure By design, SDLC

Enterprise Vulnerability Management - Patch management, Ethical Hacking

Cyber Resilience – Cyber Drills, Tabletop Exercise, Automated Red Team

Quantum Computing – Data Encryption- Rest/ Transfer

Kill Switch - Rapid Containment

Integrate Cyber Risk in the overall Risk of the Organization

Q&A

Thank You!