RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: GPS-R02

CYBER RISK LEADERS
Leadership and Influence in this Cyber-Age

Shamane Tan

Executive Advisor – APAC
Privasec
@ShamaneTan
www.linkedin.com/in/shamane

RED

RED TEAMING &
ADVANCED ETHICAL
HACKING

GRC

GOVERNANCE
AND INFORMATION
SECURITY PARTNERS

DRONE SEC

SECURITY
HACKING
HARDENING


105M

1 EXAMINING THE CISOS

THE RISE OF THE CISO

IT SUPPORT ENGINEER → SECURITY CONSULTANT → GRC MANAGER → HEAD OF INFOSEC/ DIRECTOR OF CONSULTING PRACTICE

NETWORK ENGINEER → INFRASTRUCTURE MANAGER → HEAD OF INFRASTRUCTURE → CTO

SECURITY ANALYST → IT OPERATIONS → HEAD OF INFORMATION / IT OPERATIONS MANAGER → CTO

SERVICE DELIVERY MANAGER → SECURITY MANAGER

WINTEL CONSULTANT → TECHNICAL ENG. / ARCHITECT

PROTECTIVE SECURITY → HEAD OF SECURITY

NOT ALL CISOS ARE EQUAL

Board Support

Leadership View

Reporting lines

NOT ALL CISOS ARE EQUAL

Role

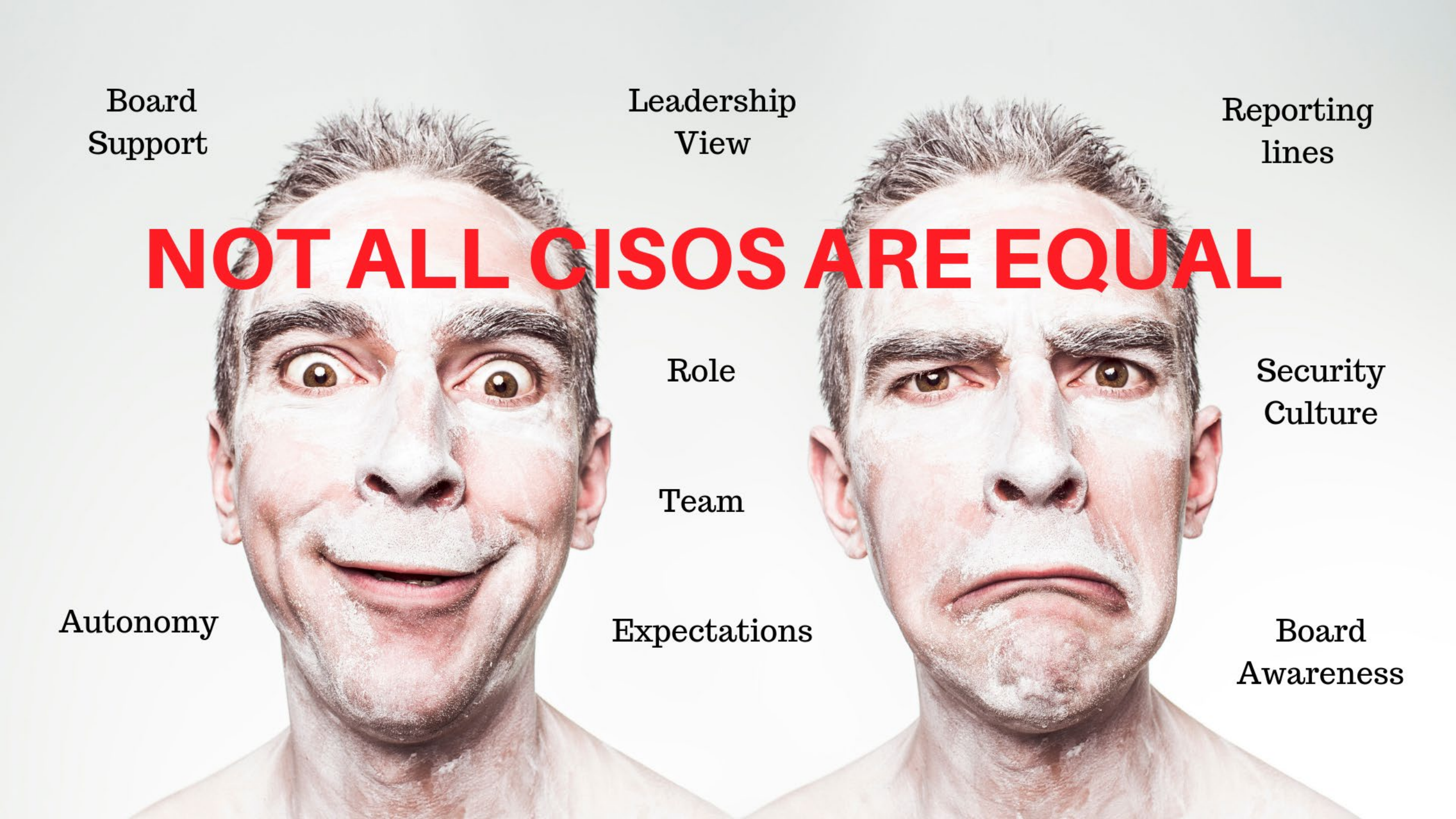
Security Culture

Team

Autonomy

Expectations

Board Awareness




IT VS. BUSINESS CISOS

Traditional Cybersecurity function that aims to have a good understanding of the business

VS.

Influential Business function that solves problems across the company

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology",
- Bruce Schneier, (2011).

"Secrets and Lies: Digital Security in a Networked World", p.9, John Wiley & Sons


Facilities
Legal
Compliance
Sales
Product
Finance
HR

2 GLOBAL PERSPECTIVES: CHALLENGES


DIGITAL
TRANSFORMATION

"Many business enterprises are still struggling with identifying a viable strategy to combat the cyber threat. It is crucial for InfoSec leaders to continue to speak and act through the lens of **risk management** in order to create a resilient response to the ongoing threats."

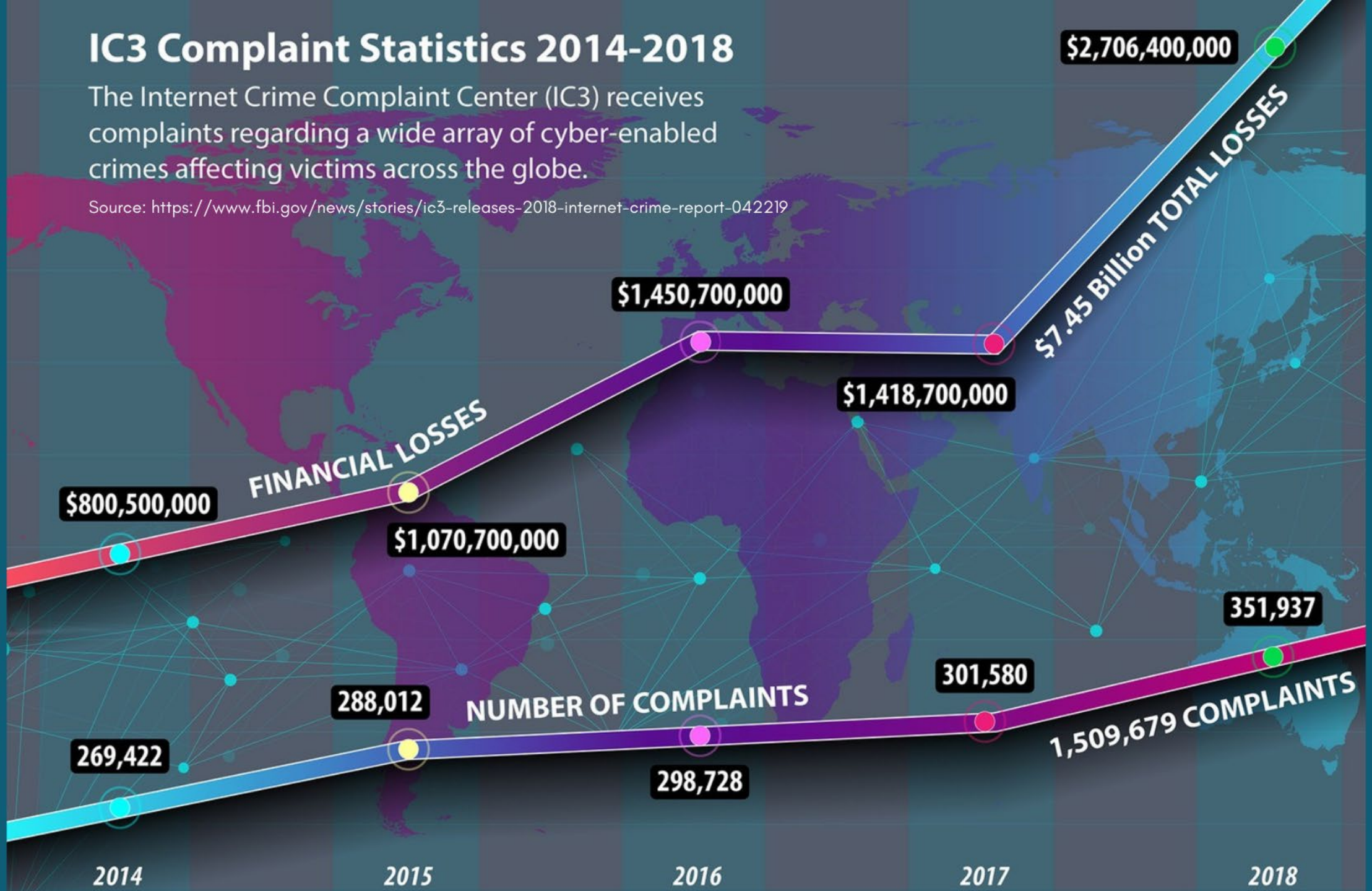
– MK Palmore, former Head of Security, FBI

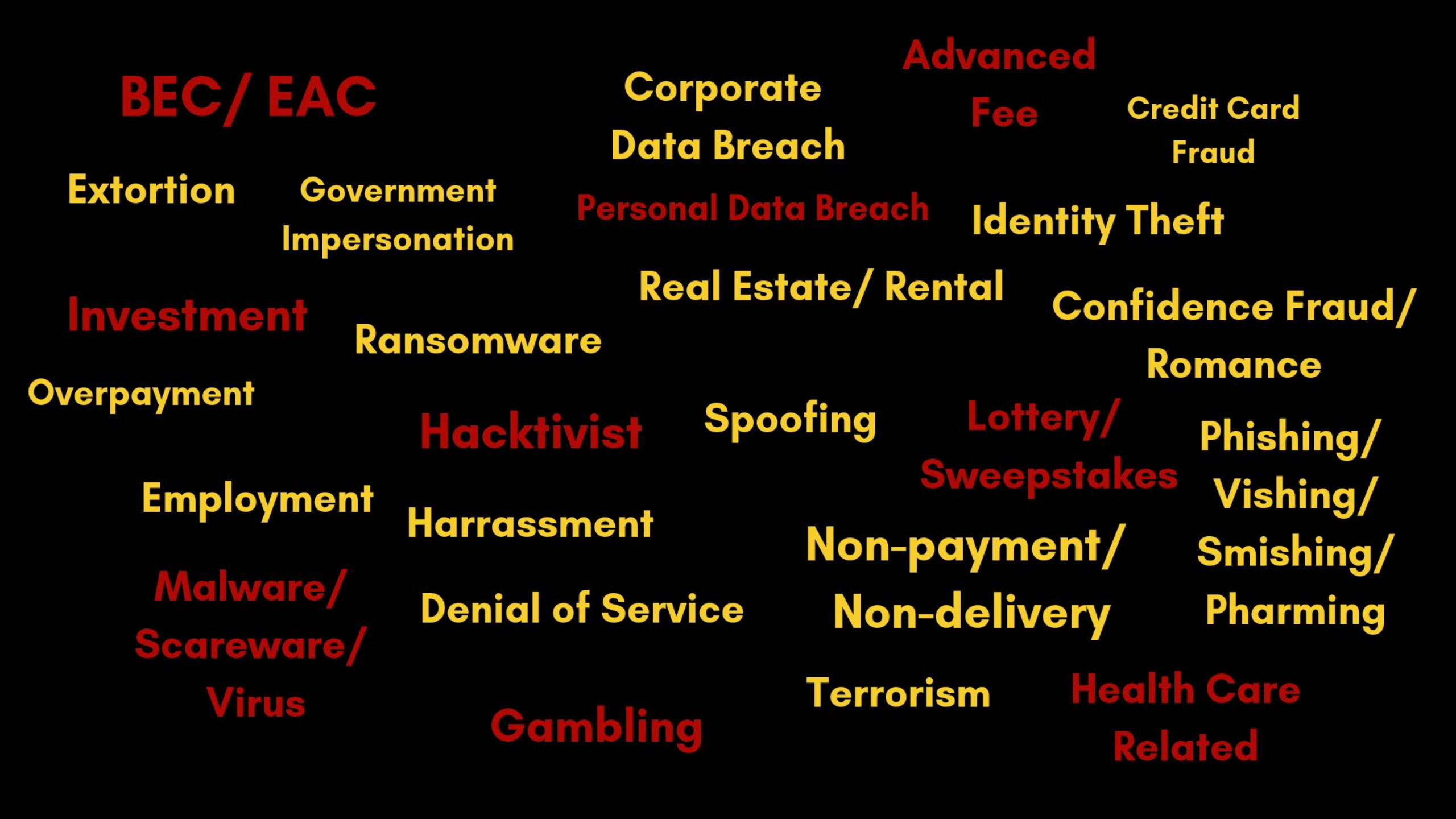

In 2018, the FBI IC3 received a total
of 351,936 complaints with losses
exceeding $2.7 Billion.

IC3 Complaint Statistics 2014-2018

The Internet Crime Complaint Center (IC3) receives complaints regarding a wide array of cyber-enabled crimes affecting victims across the globe.

Source: https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219



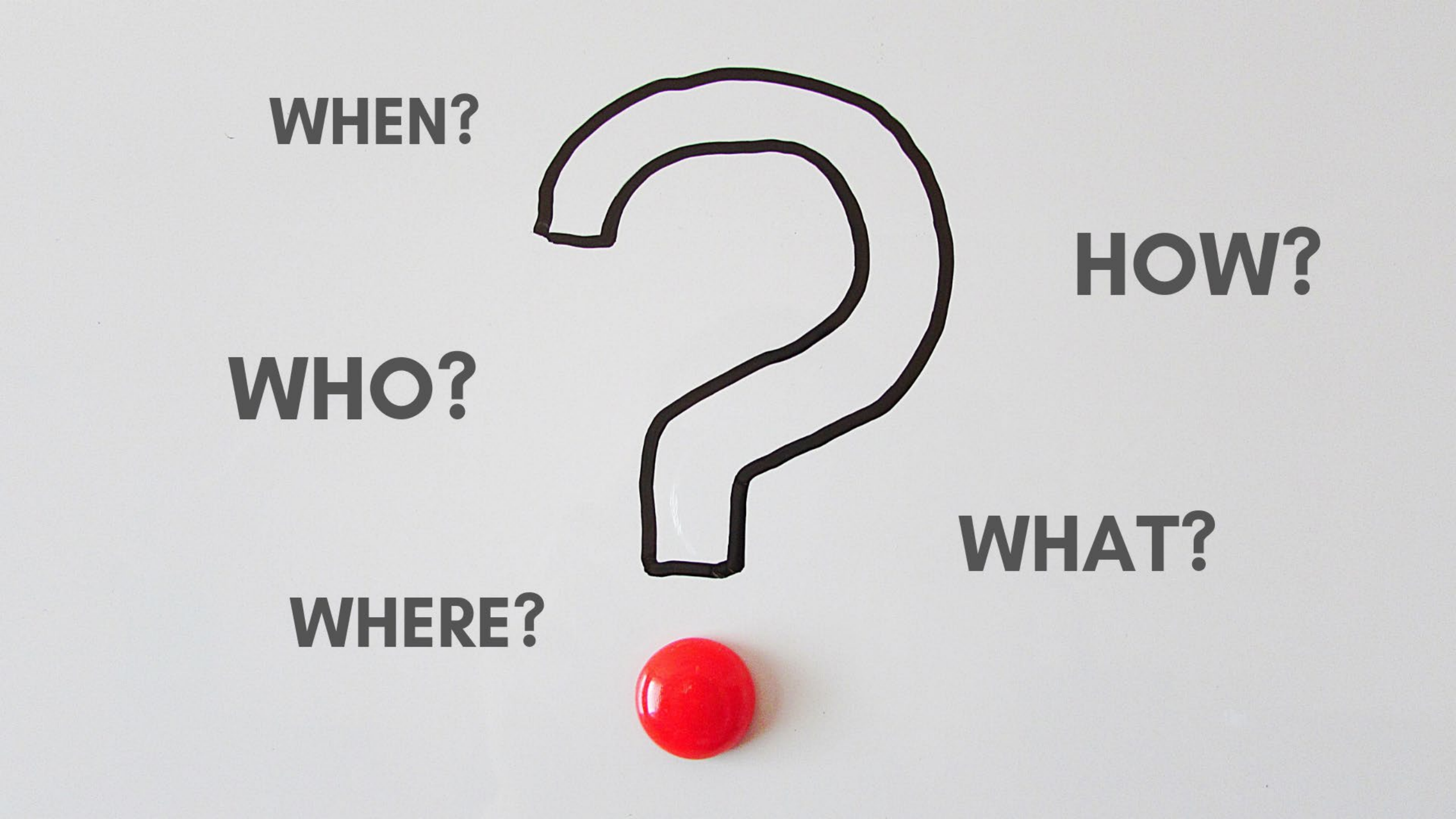

BEC/ EAC
Corporate Data Breach
Advanced Fee
Credit Card Fraud
Extortion
Government Impersonation
Personal Data Breach
Identity Theft
Real Estate/ Rental
Investment
Ransomware
Confidence Fraud/ Romance
Overpayment
Hacktivist
Spoofing
Lottery/ Sweepstakes
Phishing/ Vishing/ Smishing/ Pharming
Employment
Harrassment
Non-payment/ Non-delivery
Malware/ Scareware/ Virus
Denial of Service
Terrorism
Health Care Related
Gambling


BEC/ EAC
Corporate Data Breach
Advanced Fee
Credit Card Fraud
Government Impersonation
Personal Data Breach
Identity Theft
Investment
Ransomware
Real Estate/ Rental
Confidence Fraud/ Romance
Overpayment
Extortion
Lottery/ Sweepstakes
Spoofing
Phishing/ Vishing/ Smishing/ Pharming
Employment
Harrassment
Hacktivist
Non-payment/ Non-delivery
Malware/ Scareware/ Virus
Denial of Service
Gambling
Terrorism
Health Care Related


BEC/ EAC
Corporate Data Breach
Advanced Fee
Credit Card Fraud
Confidence Fraud/ Romance
Personal Data Breach
Identity Theft
Real Estate/ Rental
Government Impersonation
Investment
Non-payment/ Non-delivery
Extortion
Overpayment
Lottery/ Sweepstakes
Phishing/ Vishing/
Spoofing
Employment
Harrassment
Hacktivist
Ransomware
Smishing/ Pharming
Malware/ Scareware/ Virus
Denial of Service
Gambling
Terrorism
Health Care Related

SUPPLY CHAIN RISK

- Vendors security hygiene
- Type of information being disclosed to 3rd parties
- Due diligence to check adherence to Security policies
- Contractual arrangements
- Business continuity in the event of a disaster
- Certifications
- Alignment of assessments and controls
- Regular annual review


WHEN?
HOW?
WHO?
WHAT?
WHERE?

"Only amateurs attack machines; professionals target people"
- Bruce Schneier, (2011).

Semantic Attacks: The Third Wave of Network Attacks. Schneier on Security blog.

HUMAN FACTOR

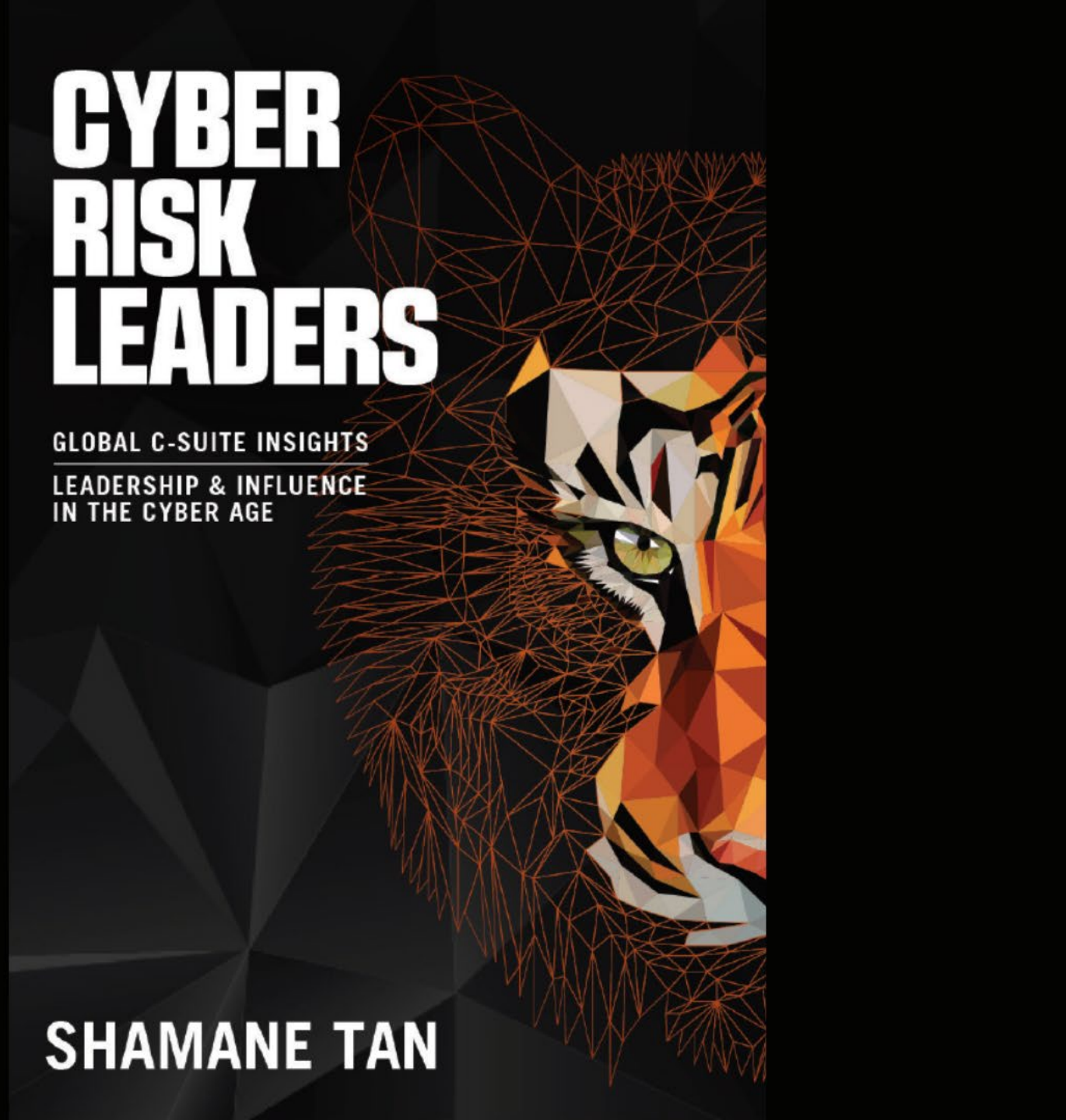
UNINTENTIONAL
UNAWARE
VS.
MALICIOUS
INSIDER THREAT

“Working under a leadership who is abusive and untrustworthy ‘activates’ *underlying and dormant traits of exploitative self-interest*. This leads to increasing manipulation, control and frankly unethical behaviour.”

Rebecca Greenbaum, Scott Dust, Christian J. Resick, Jaclyn A. Margolis, Mary Bardes Mawritz (Ethical leadership and employee success: Examining the roles of psychological empowerment and emotional exhaustion, 2017)

If you were to perform the perfect crime to get back at our company, what would you do, and how?

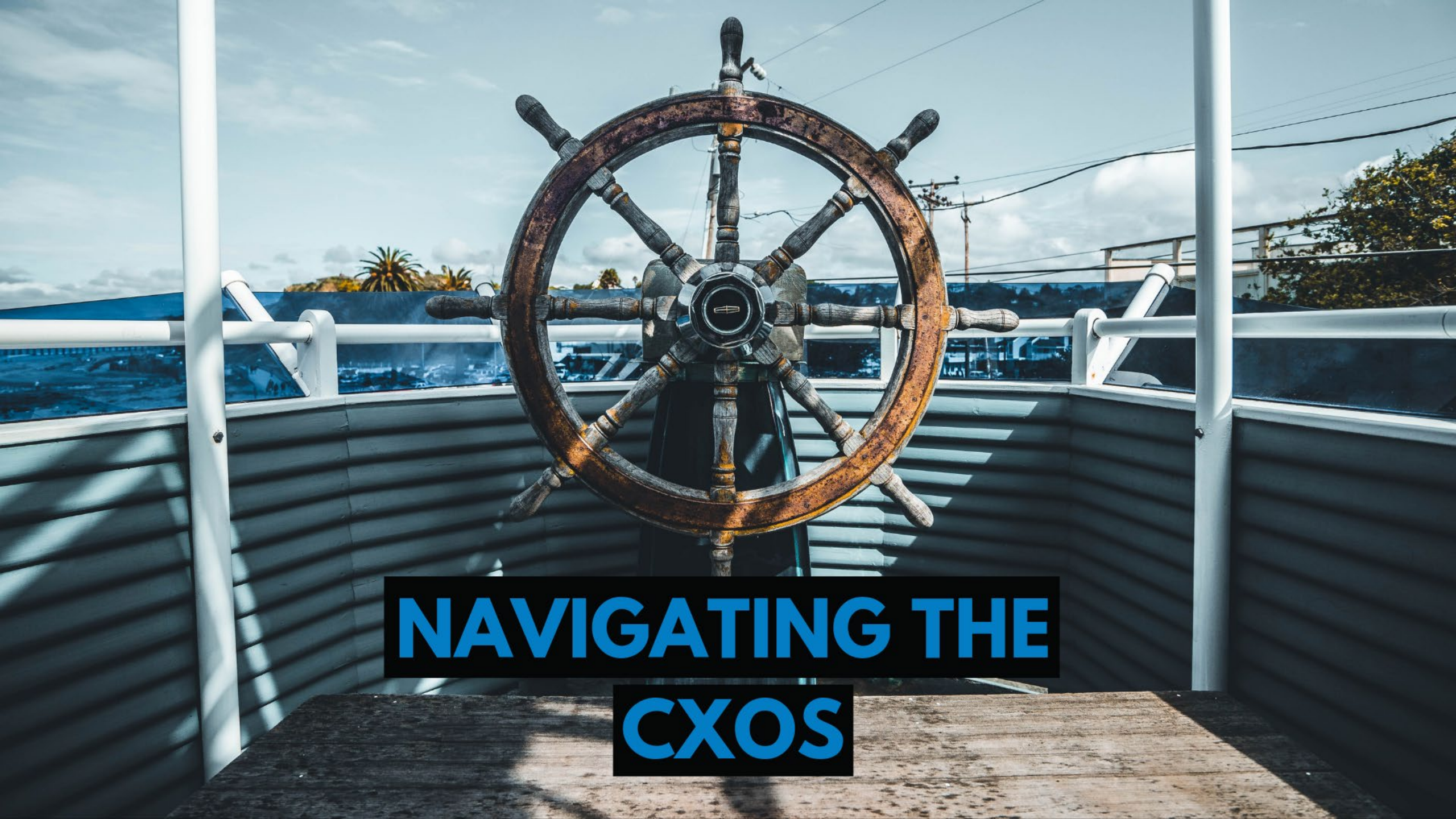
3 CISO INSIGHTS



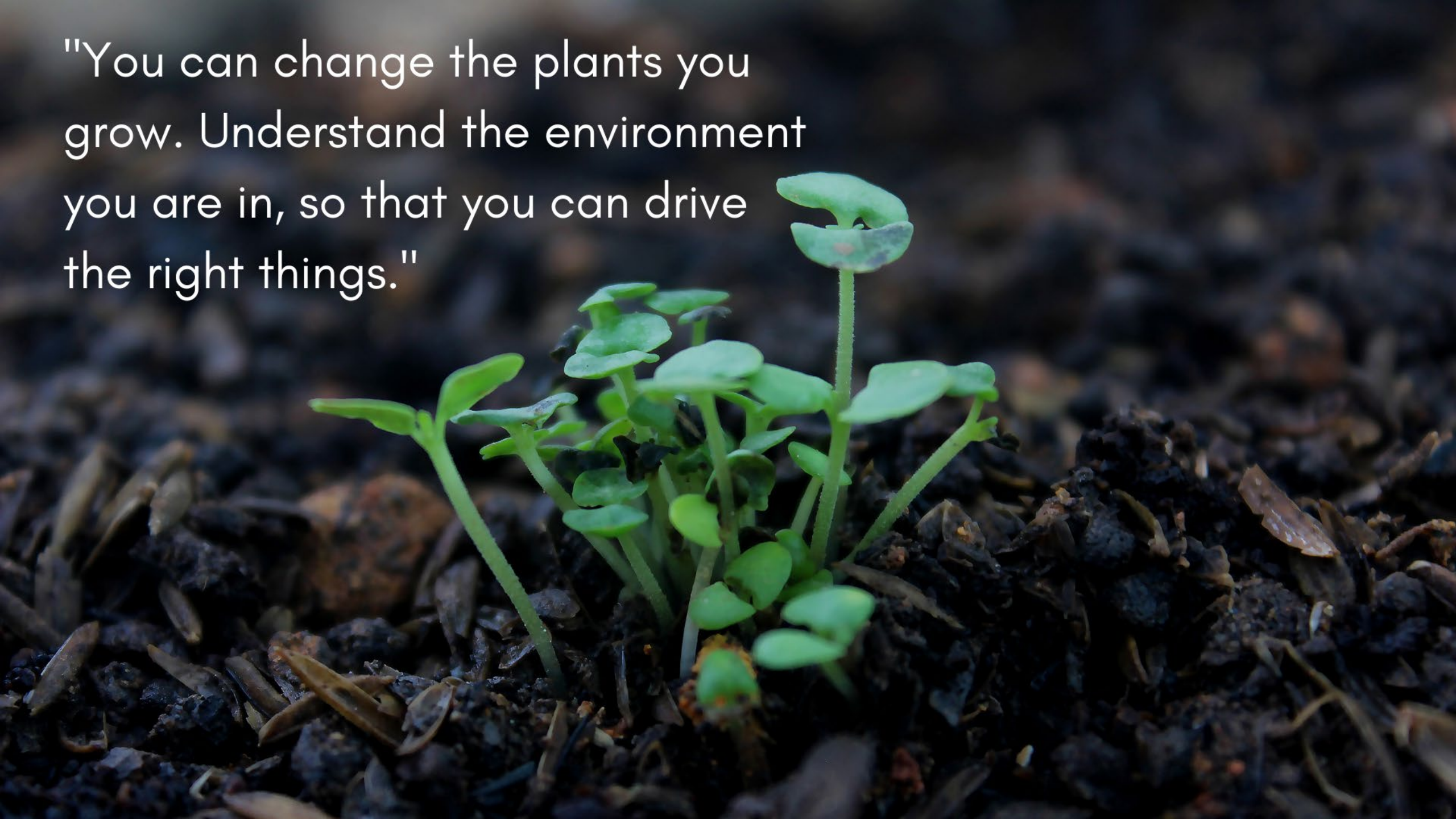
UK, US, ISRAEL, SINGAPORE, AUSTRALIA

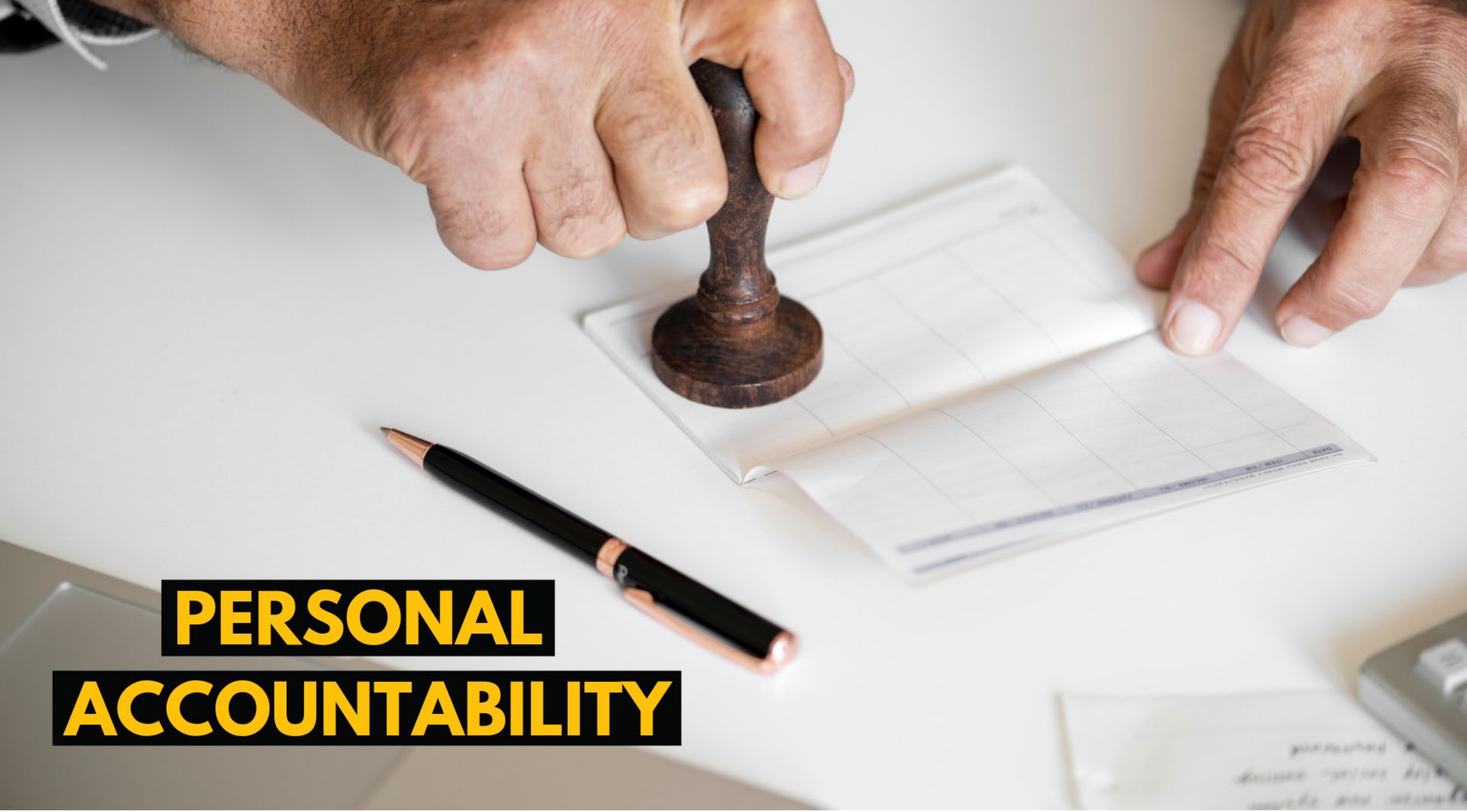
GETTING THE ATTENTION OF THE BOARD


THE ART OF
STORYTELLING


NAVIGATING THE
CXOS

The key element is that at the CEO or group CEO's table, you need to have as many advocates as possible to sustain your influence.


"You can change the plants you grow. Understand the environment you are in, so that you can drive the right things."


PERSONAL
ACCOUNTABILITY


Moody's Analytics has already started using its credit-rating expertise to evaluate organizations on their risk to a major impact from a cyberattack.


DEALING WITH
INTELLIGENCE

Threat Intelligence & Analysis

80% of organisations

Understand the threats and risks against the organisation using internal and external information sources

Blue Team

Consumers of Intelligence

Threat Hunting

20% of organisations

Pro-actively searching for attackers and malware in your organisation based on informed hypothesis

Red Team

Producers of Intelligence


PURPLE
TEAMING

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		

KEY TAKEAWAYS

FOR OUR CYBER RISK LEADERS

#1 FIND BUSINESS-SIDE CHAMPIONS

KEY TAKEAWAYS

FOR OUR CYBER RISK LEADERS

#2 BRING THEM ON A JOURNEY

KEY TAKEAWAYS

FOR OUR CYBER RISK LEADERS

#3 MANAGE RISK, DON'T ADMIRE IT

KEY TAKEAWAYS

FOR OUR CYBER RISK LEADERS

DEMONSTRATE HOW SECURITY ENABLES

THANK YOU

Shamane Tan, Executive Advisor - APAC
shamane.t@privasec.com
www.linkedin.com/in/shamane
@ShamaneTan

Shamane Tan

Executive Advisor - APAC at
Privasec | Cyber Risk Meetup Fou...