

RSA®Conference2015

Singapore | 22-24 July | Marina Bay Sands

SESSION ID: GRM-R02

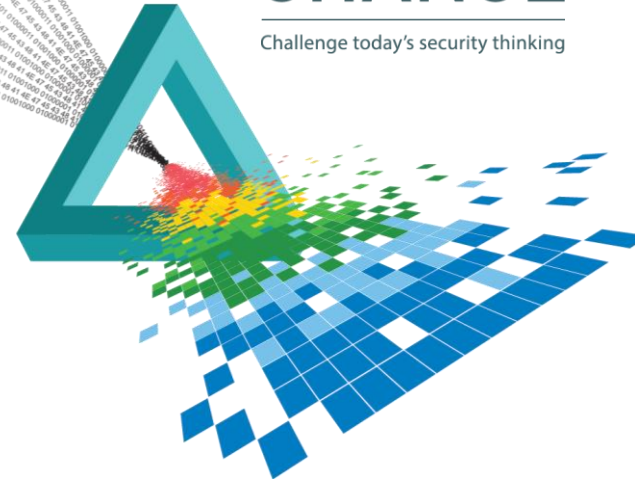
Hiring the right person for the most challenging security role of all

David Siah

Country Manager
Trend Micro

CHANGE

Challenge today's security thinking



Why a CISO is needed in the organization?



WORLD
ECONOMIC
FORUM

Cyber attacks are one of the **TOP**

5 RISKS



The Institute of
Internal Auditors

86% of board of directors are not
actively involved in cybersecurity
preparedness



Harvard
Business
Review

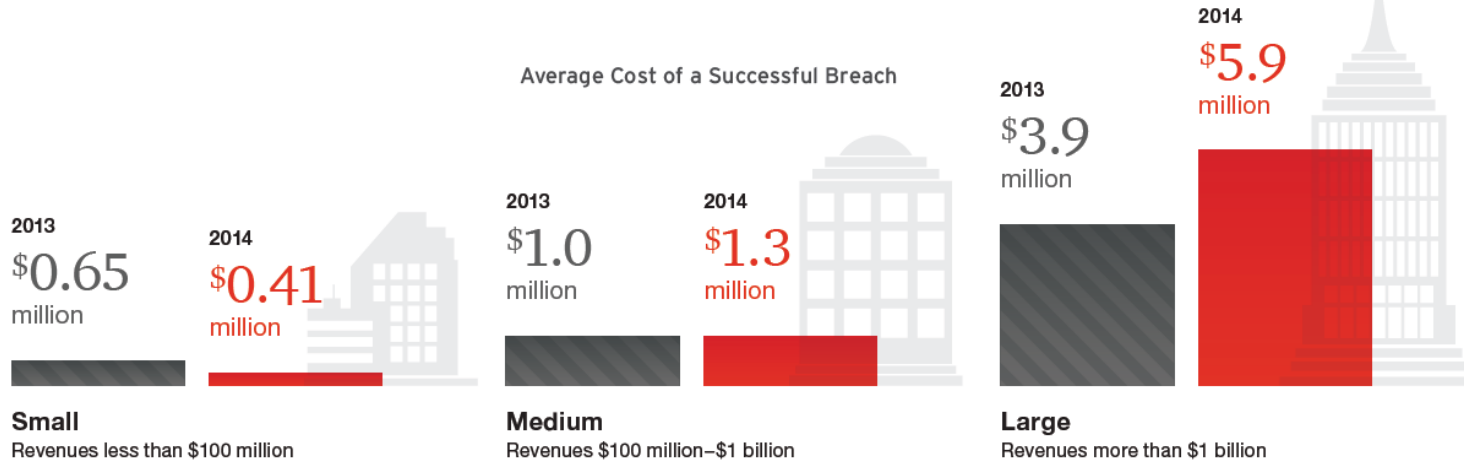
60%

IT/Sec
concerned

70%

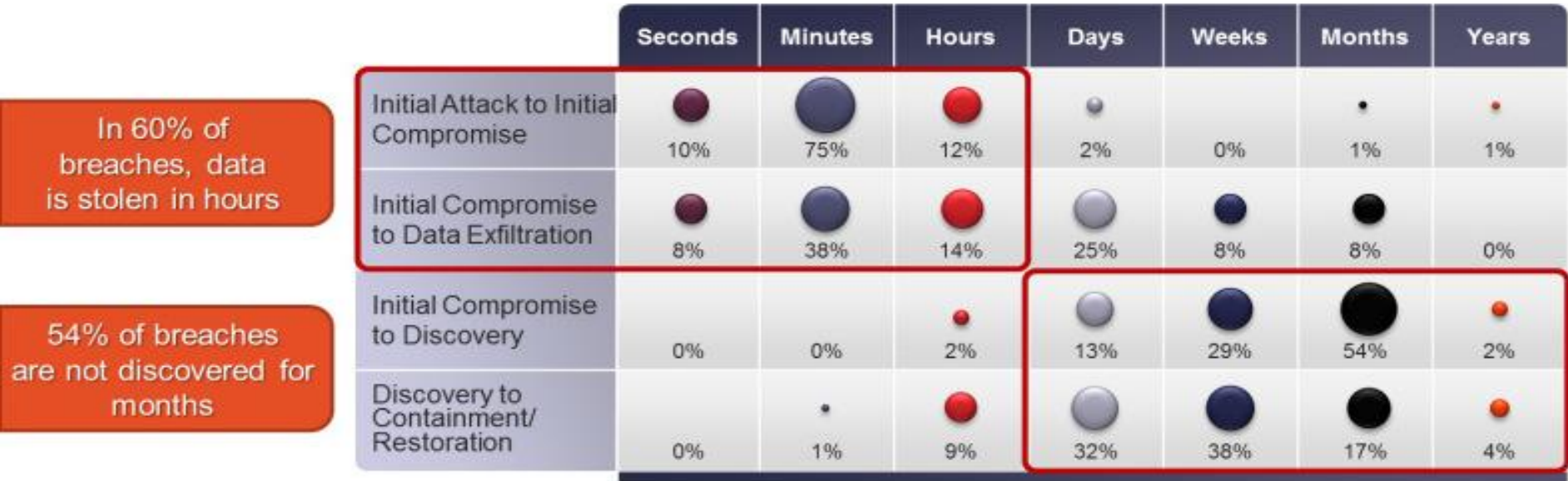
decision makers
uninformed of risks

Why a CISO is needed in the organization?



PricewaterhouseCoopers, the Global State of Information Security® Survey 2015

The Data Breaches

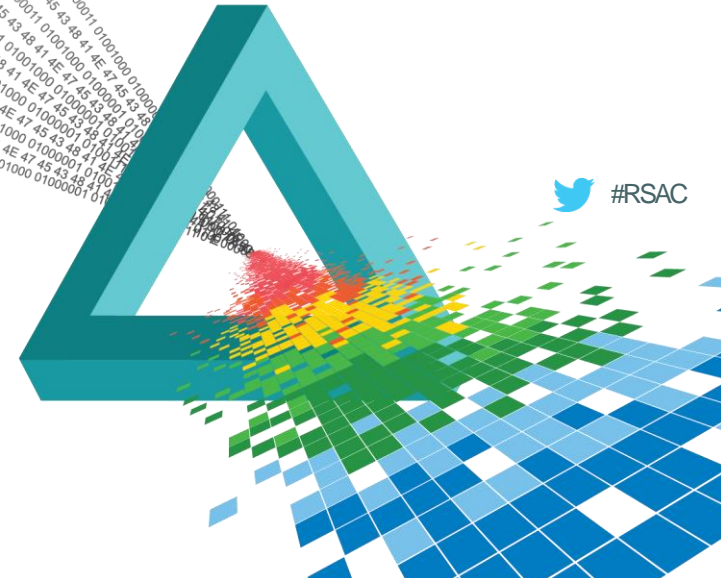


Timespan of events by percent of breaches

RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

Survey of 200 Global CxO June 2015



Threat Source:

Rank these threats to your organization

33% Insider threat

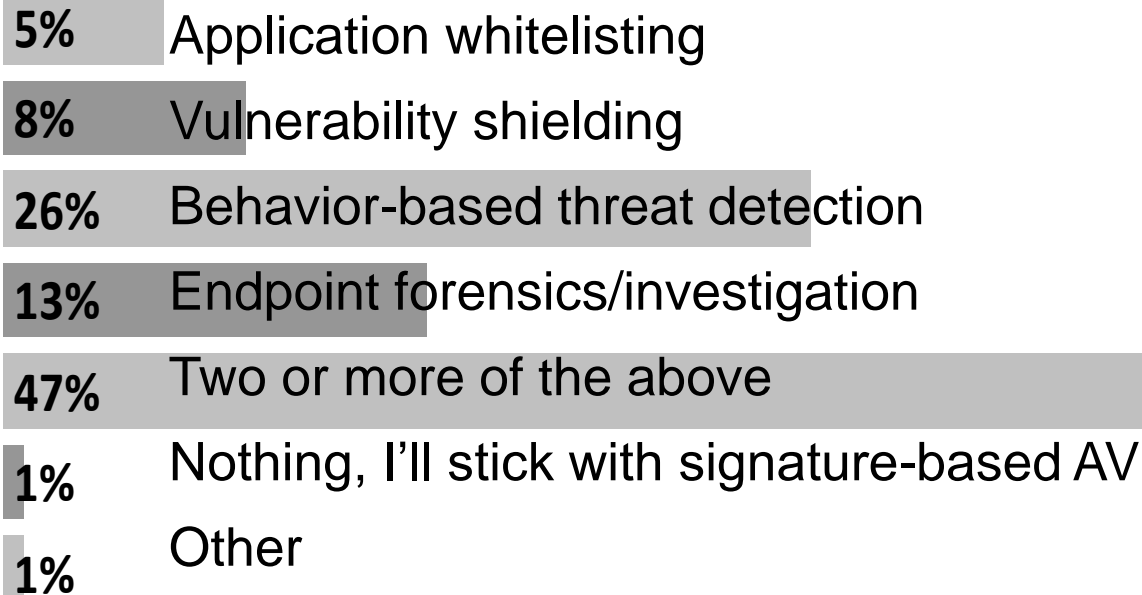
13% Activist / hacktivist

45% Cyber-criminals

10% Cyber-espionage

Endpoint Modernization

Beyond signature-based AV on your endpoints, what additional approach is most interesting:



CISO:

Does your organization have a Chief Information Security Officer (CISO)?

28% Yes, he/she reports to the CIO

25% Yes, he/she reports elsewhere

47% No

Board Visibility into Security

How much visibility does your Board of Directors have into your security initiatives?



Targeted Attacks:

How would you rate your organization's overall ability to detect and stop a targeted attack?



Cybersecurity Skills Crisis

Too Many Threats

 **62%**
INCREASE
IN BREACHES
IN 2013¹

1 IN 5 
ORGANIZATIONS
HAVE **EXPERIENCED**
AN APT ATTACK⁴

US \$3
TRILLION
TOTAL GLOBAL
IMPACT OF
CYBERCRIME³

 **8 MONTHS**
IS THE AVERAGE TIME
AN ADVANCED THREAT
GOES UNNOTICED ON
VICTIM'S NETWORK²

2.5
BILLION 
EXPOSED RECORDS AS
A RESULT OF A DATA BREACH
IN THE PAST 5 YEARS⁵

Too Few Professionals

 **62%**
OF ORGANIZATIONS
HAVE NOT INCREASED
SECURITY TRAINING
IN 2014⁶

 **1 OUT OF 3**
SECURITY PROS ARE
NOT FAMILIAR WITH
ADVANCED PERSISTENT
THREATS⁷

 **<2.4%**
GRADUATING STUDENTS
HOLD COMPUTER
SCIENCE DEGREES⁸

 **1 MILLION**
UNFILLED SECURITY
JOBS WORLDWIDE⁹

83% 
OF ENTERPRISES CURRENTLY
LACK THE RIGHT SKILLS AND
HUMAN RESOURCES TO PROTECT
THEIR IT ASSETS¹⁰

Enterprises are under siege from
a rising volume of cyberattacks.

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

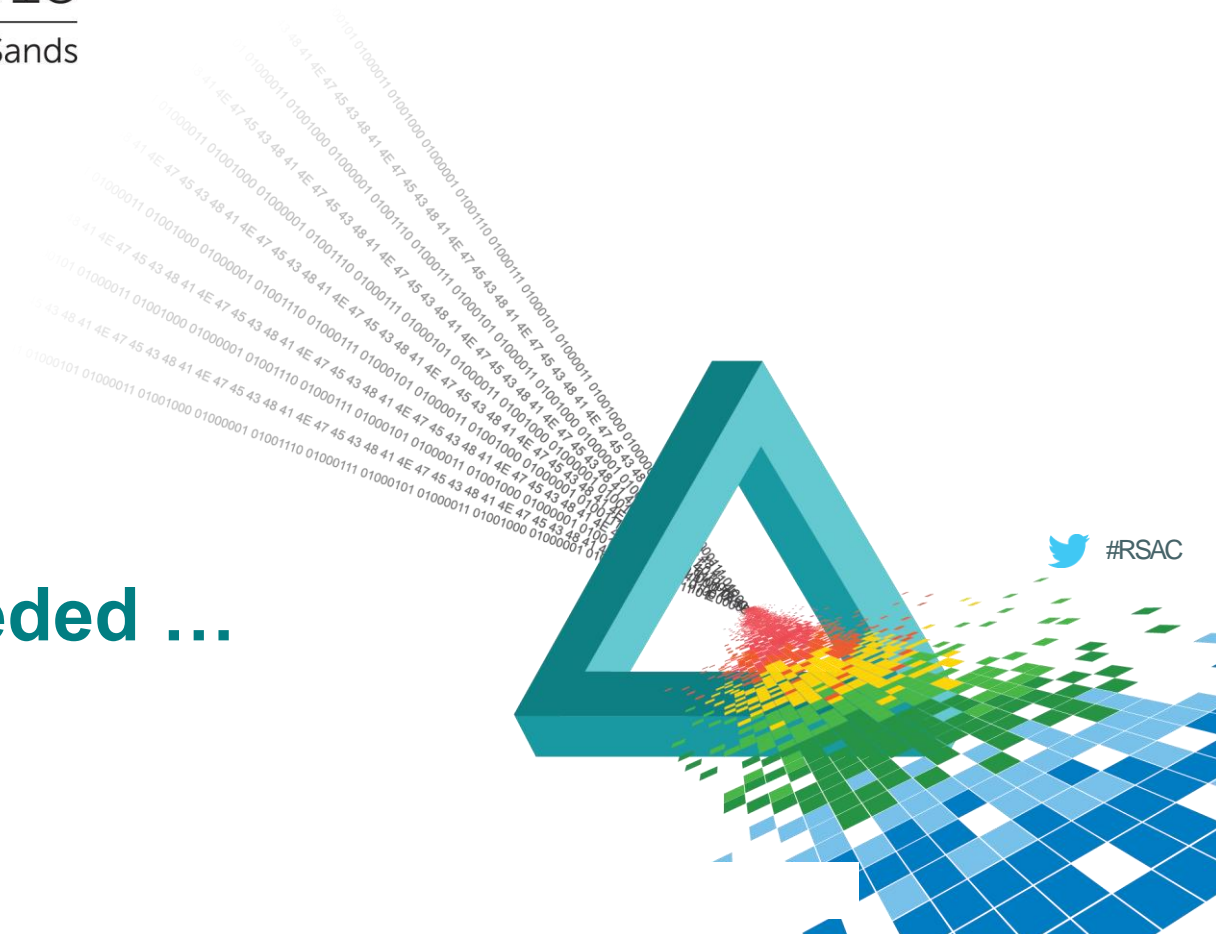
SOURCES: 1. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; 2. *M-Trends 2013: Attack the Security Gap*, Mandiant, March 2013; 3. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; 4. *ISACA's 2014 APT Study*, ISACA, April 2014; 5. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; 6. *ISACA's 2014 APT Study*, ISACA, April 2013; 7. *ISACA's 2014 APT Study*, ISACA, April 2014; 8. *Code.org*, February 2014; 9. *2014 Cisco Annual Security Report*; 10. *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014



RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

The skill sets needed ...



Understand the Business



Risk Management and Governance

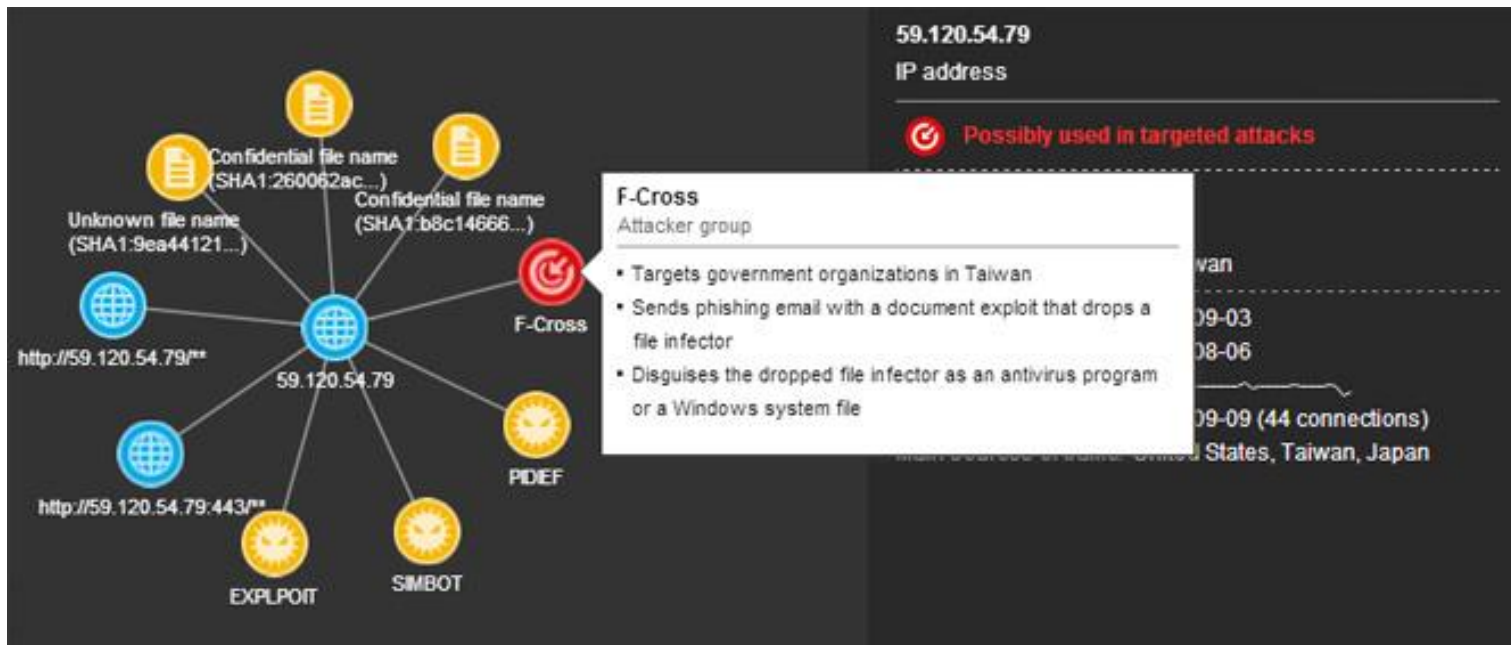


Understand contracts and their implication

Contracts, SLAs and Cloud Security

The Weak Link?

Intelligence and identifying new and emerging threats... #RSAC




Weapons Grade Arsenal

- ◆ **Greater** reconnaissance
- ◆ Utilization of 0-days
- ◆ Undetectable by anti-virus
- ◆ Able to withstand normal disinfection methods like reinstalling OS
- ◆ Calling home is undetected by DLPs and IPS/IDS
- ◆ Data extraction across an air gap

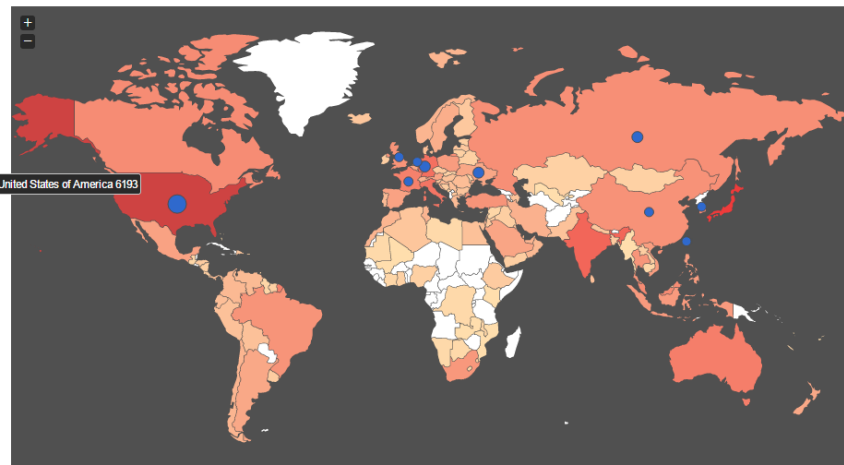


Command & Control Communications



Senna *CnC* Potal 


Map of Total Region Census – Active Endpoints of CnC within the last 7 days:




Week 50

Count of Region Census 

Country Code	Endpoint Count
JP	7405
US	6193
TW	4120
IN	2179
DE	1520

Country Count of Top CnC Site 

Country Code	CnC Site Count
US	387
UA	78
RU	74
DE	59
KR	50

Top Malware Family 

Name	Server	Victim
trojan	143	1505
rodecap	103	293
gozeus	50	118
zeus	47	278
qe	42	945

Common Traits

- Uses typical protocols (HTTP)
- Uses legitimate sites as C&C
- Uses internal systems as C&C
- Uses 3rd party apps as C&C
- May use compromised internal systems

Advantages

- Maintains persistence
- Avoids detection

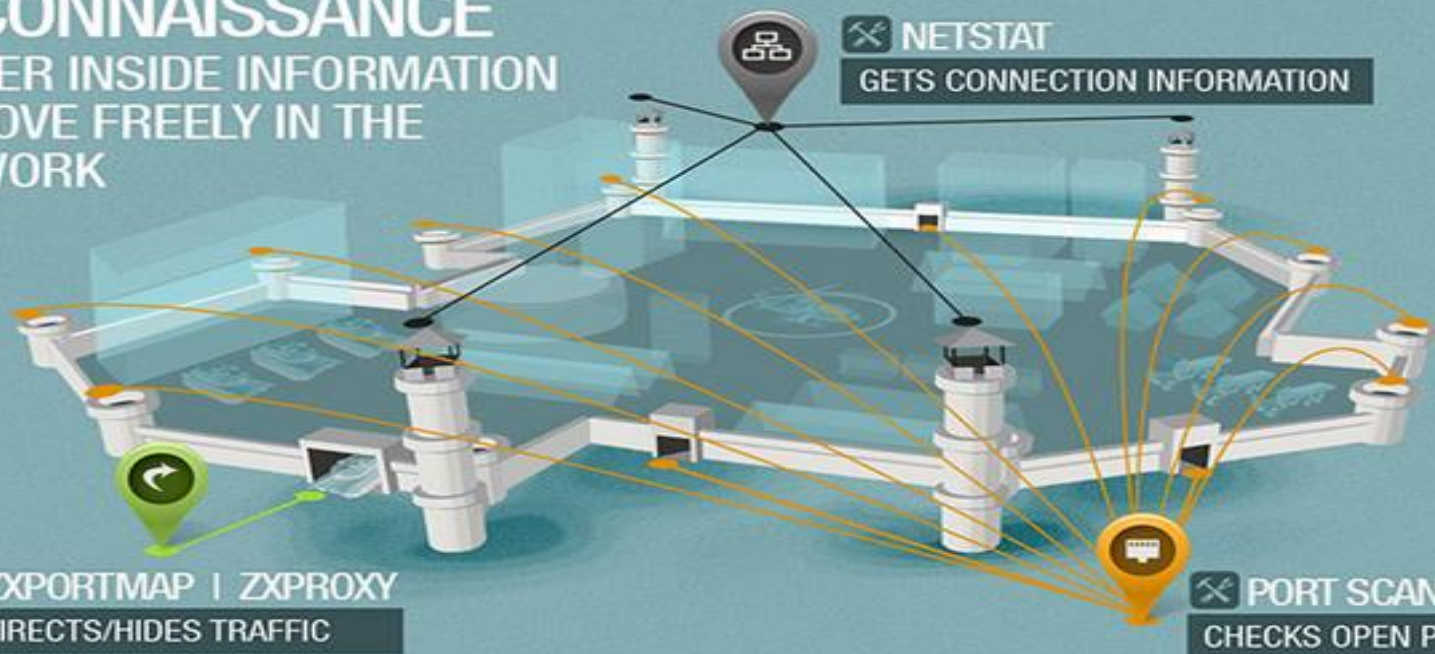
**54% of C&C Lifespan
< 1 Day**

LATERAL MOVEMENT TACTICS

AFTER IT GATHERS INFORMATION, GAINS ENTRY, AND ESTABLISHES COMMAND-AND-CONTROL INSIDE A TARGET NETWORK, APTs MOVE Laterally TO EXFILTRATE SENSITIVE DATA.

RECONNAISSANCE

GATHER INSIDE INFORMATION TO MOVE FREELY IN THE NETWORK



CREDENTIALS STEALING

STEAL LEGITIMATE CREDENTIALS TO HACK INTO OTHER COMPUTERS

HOOKING

INTERCEPTS AND RECORDS PASSWORDS

KEYLOGGER

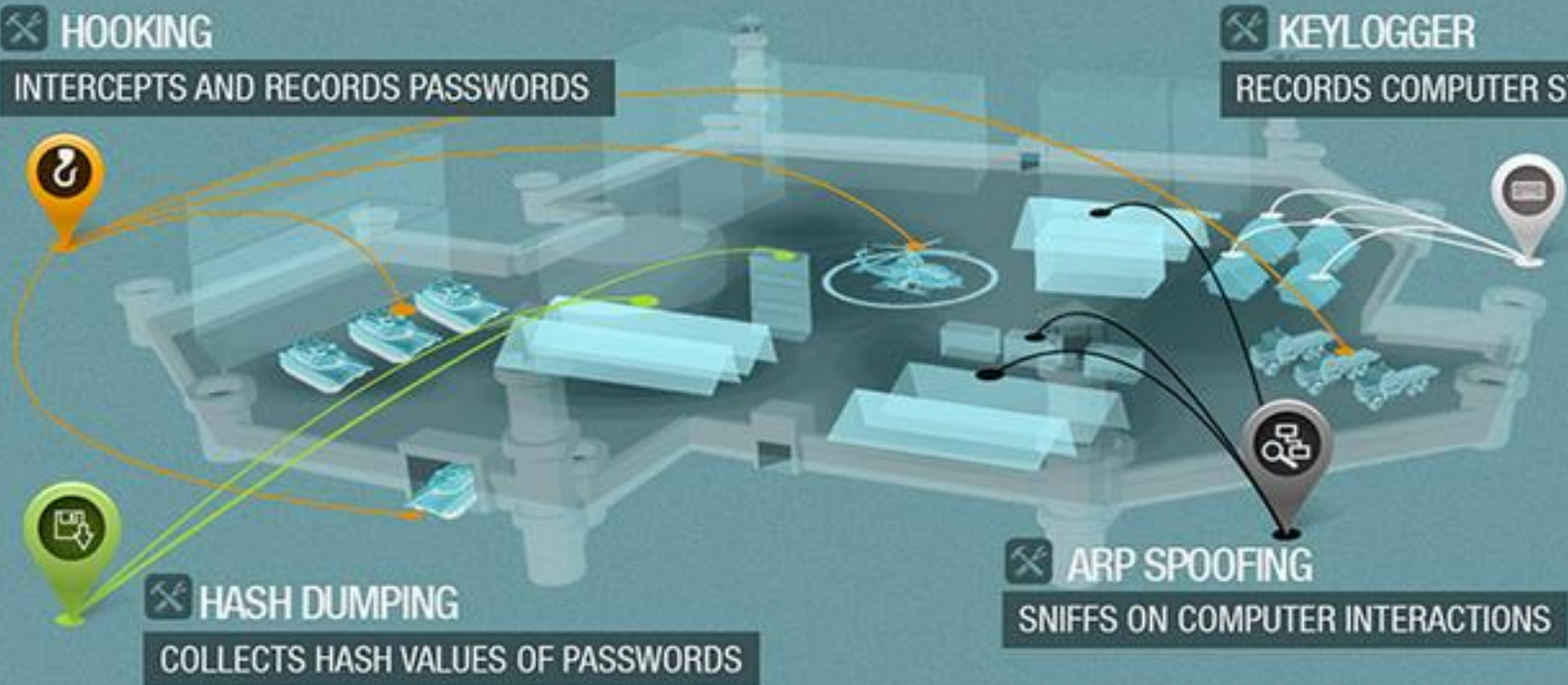
RECORDS COMPUTER STROKES

HASH DUMPING

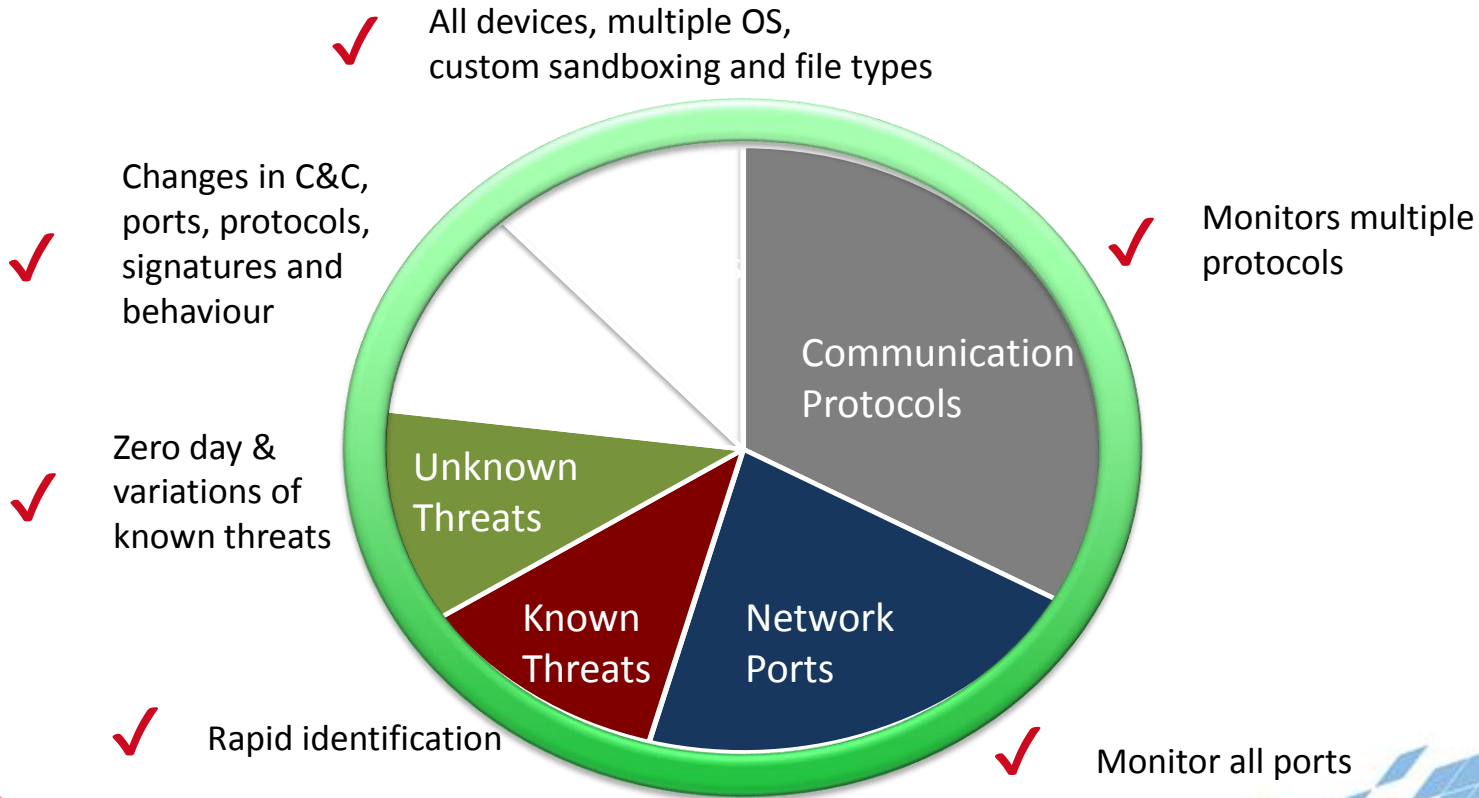
COLLECTS HASH VALUES OF PASSWORDS

ARP SPOOFING

SNIFFS ON COMPUTER INTERACTIONS

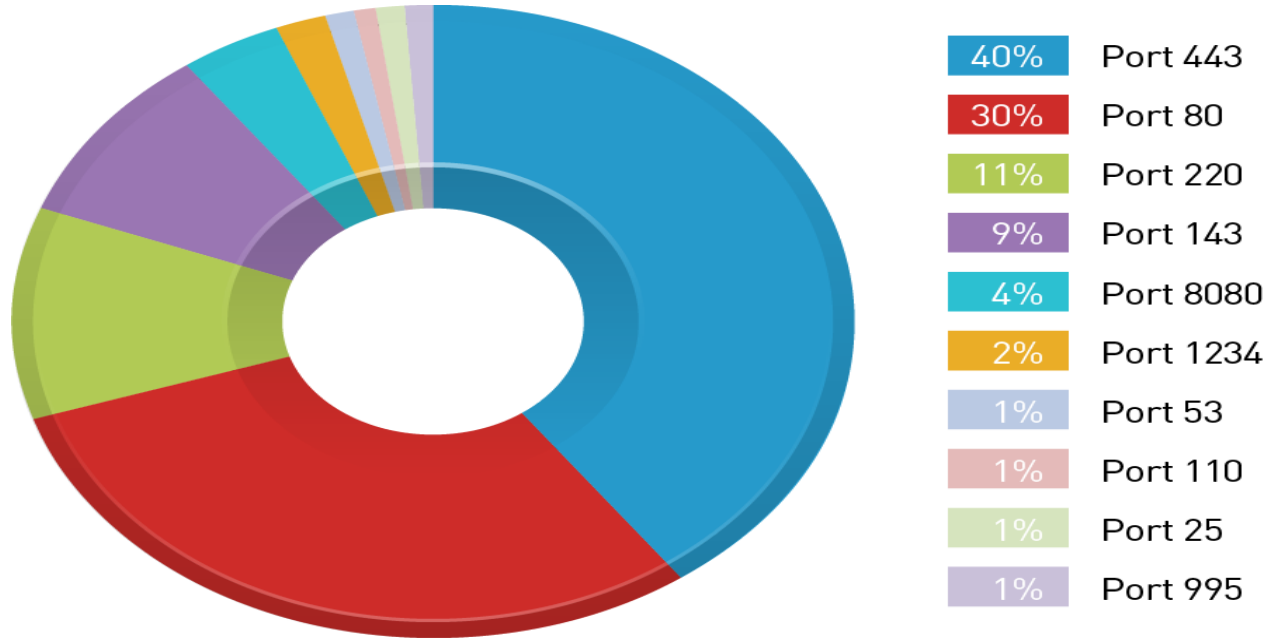


Situation Awareness



Situation Awareness

Ports used by PoisonIvy malware 2008-2015



What's in Your Organization?

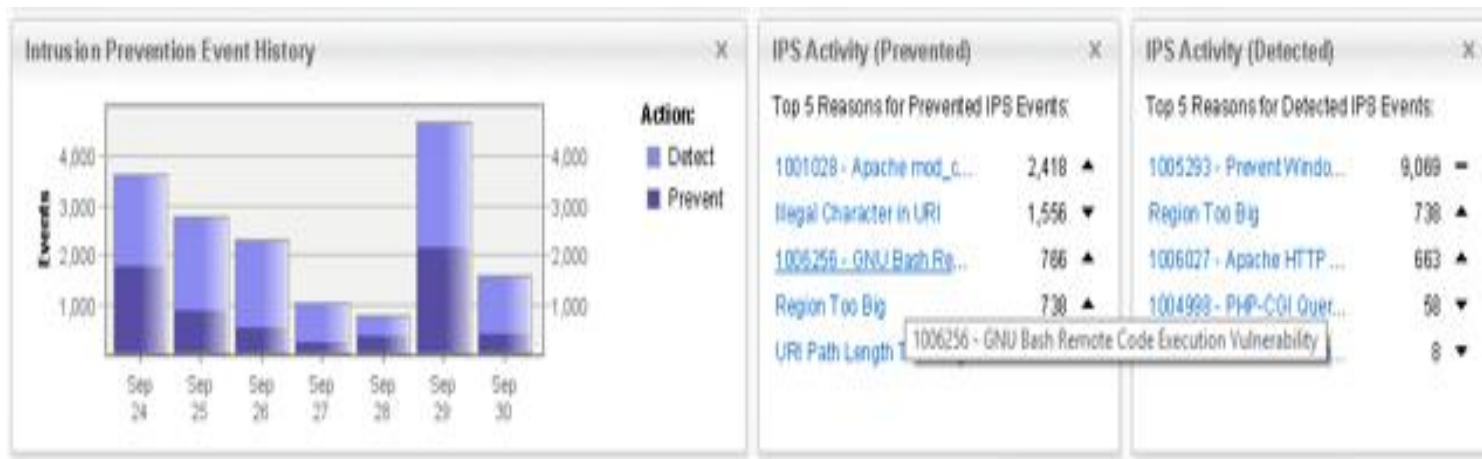
Sample Threat Types Detected	Presence
Advanced malware	98%
Active botnet	94%
Disruptive applications	88%
Banker malware	75%
Malicious documents	75%
Zero-day malware	49%
Network attacks	84%
Android malware	28%



Source: Real-life proof-of-concept sample results
(conducted by Trend Micro technical team in 2014)

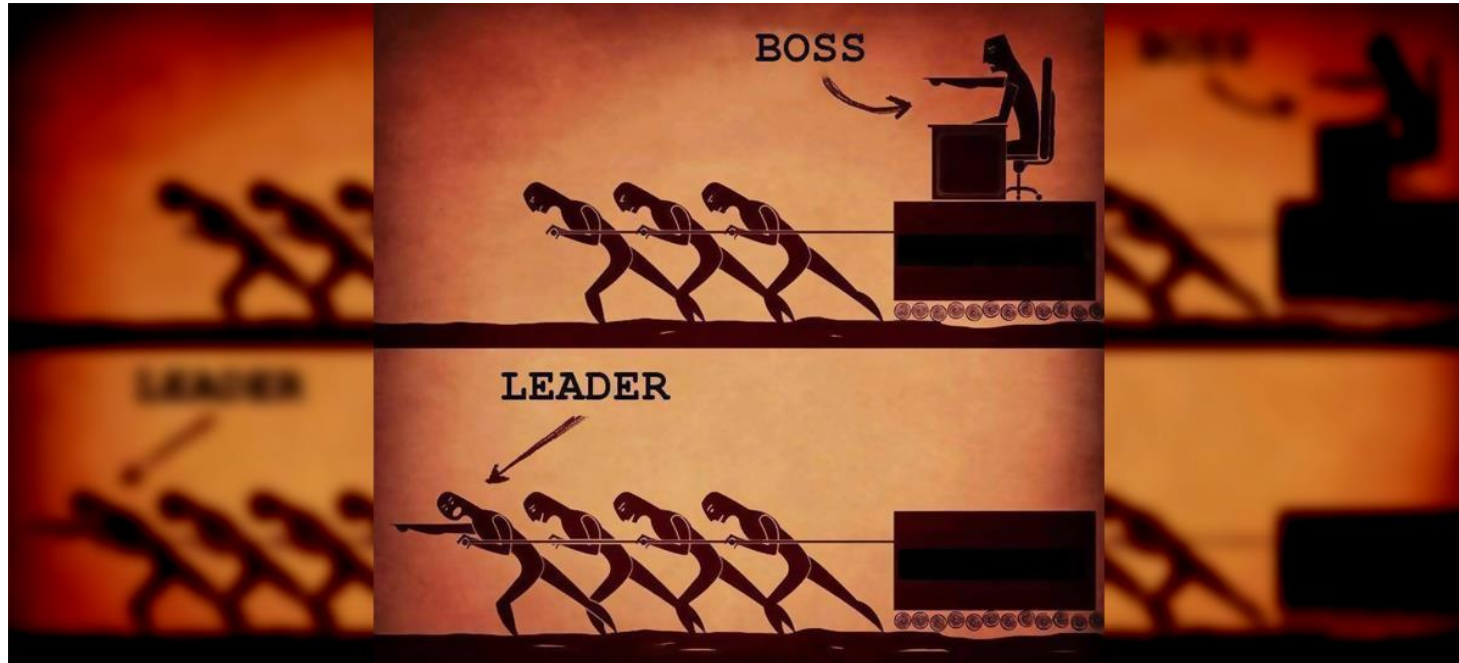
(0 day) Vulnerabilities leads to (0day) Exploits

- ◆ 5 days after ShellShock: 766 attacks attempted (example)



- ◆ On Sept 30th, at a company managing 100+ servers. Five days after the vulnerability was made public.
- ◆ Other Similar Cases: HeartBleed, MS08-067 (SMB/Conficker)

Leadership



Key skills checklist

- ❑ Understand the business
- ❑ Possess key business skills including risk management and governance
- ❑ Communicate with the board in a language they understand
- ❑ Understand contracts and their security implications, i.e., with cloud service providers, outsourcers, etc. They need to find security issues during the negotiation process and point them out to key stakeholders such as the legal department
- ❑ Identify new and emerging threats and the technologies to deal with them
- ❑ Show leadership – be proactive in planning information security projects and have a clear vision for the department

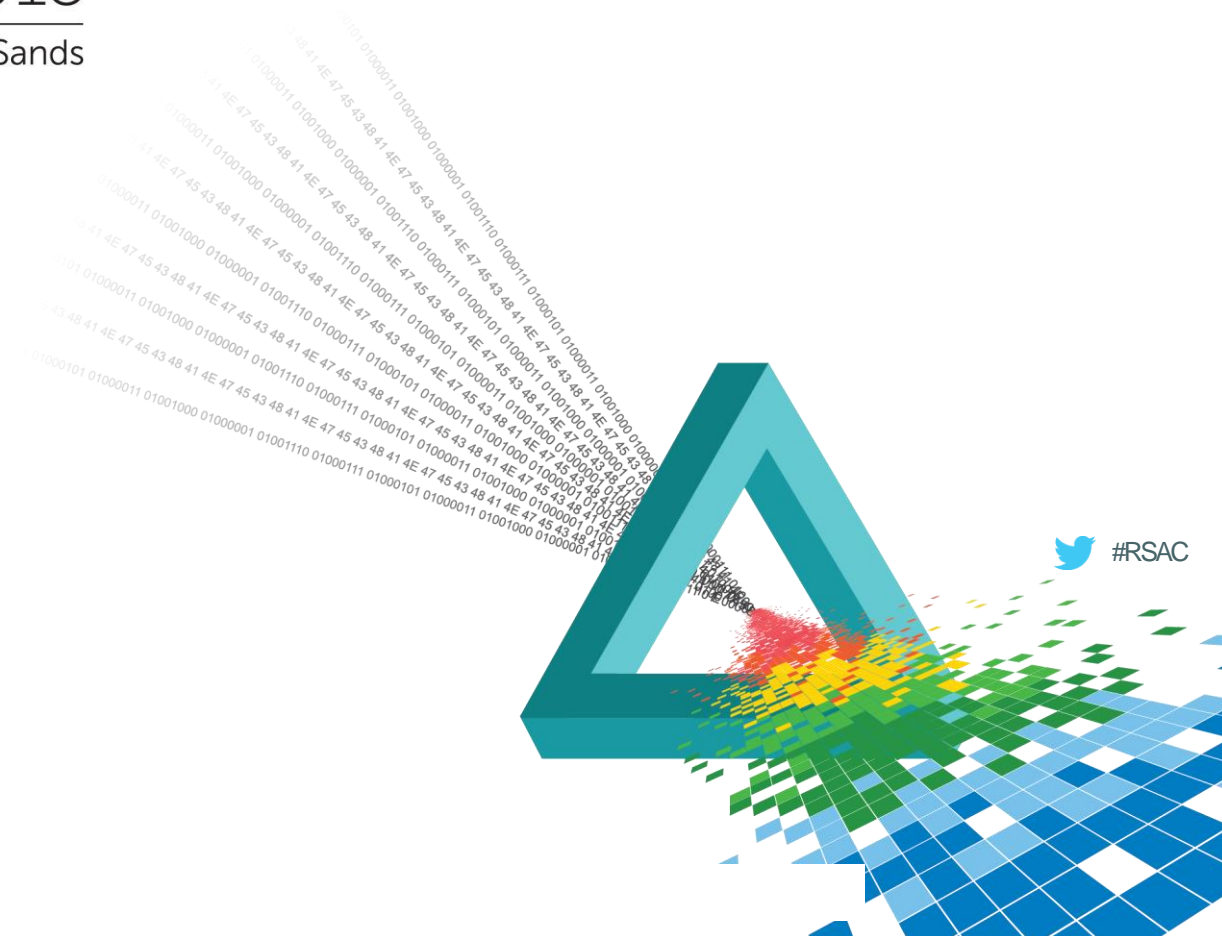
Problem solved?



RSA[®]Conference2015

Singapore | 22-24 July | Marina Bay Sands

Thank you



Abstract Recap

- ◆ There have been a huge spate of cyber-attacks recently such as the hacking on Malaysia Airlines. What is clear is that the role of the Chief Information and Security Officer (CISO) is becoming more crucial as security becomes ever more mission critical for business continuity in this era of the Internet of Everything. As the value of sensitive data to organisations and cybercriminals increase, so has the importance of the CISO, in a way barely even imagined a decade ago.
- ◆ However, given continued skills shortage in the industry, the problem for firms is finding the right person to fit the job – making CISOs hard to find and even harder to keep once their reputation grows. The CISO is now a highly strategic role which has the power to set the tone and vision for information security investments and roadmaps.
- ◆ In this talk, David will help outline what exactly constitutes the right person for the role of CISO and what are the crucial attributes a CISO should have. Some of these include:

- ◆ Understanding the business and possessing key business skills including risk management and governance. Think about and understand the business objectives and the strategic direction, and how information security enables all this to happen
- ◆ Intelligence gathering and analysis:
 - ◆ Collecting intelligence and analysis will help the organization when it comes to reacting to a breach. This also allows the CISO to outline the impacts of the breach in terms of hard cost and soft cost.
- ◆ Business Communication Skills
 - ◆ Ensure security updates are digestible and easy to understand. It is also worth summarizing it into a short and easy to read report for busy executives, such as the CEO.
 - ◆ Not forgetting the other employees, language should be weaved into clear policies for them to understand, abide by, and educate.
- ◆ Understanding contracts and their security implications, i.e., with cloud service providers, outsourcers, etc.
- ◆ The CISO needs to find security issues during the negotiation process and point them out to key stakeholders such as the legal department.
- ◆ Identifying new and emerging threats and the solutions to deal with them
- ◆ Organizational Leadership