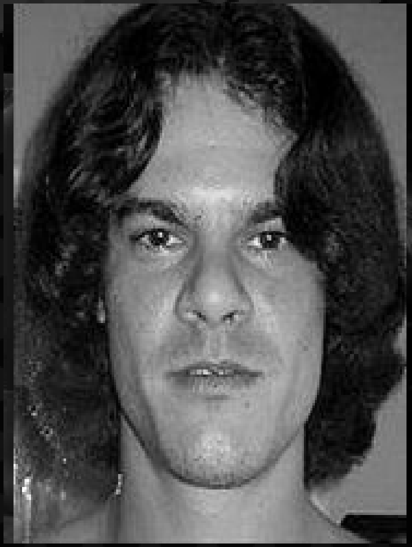
Emerging Security Disciplines

Sangameswaran.M.V. - GSEC, CISSP

Regional Manager – System Engineering
Principal Compliance & Incident Management Specialist – Asia

symantec.

Sources Of A Breach



Organized
Criminal

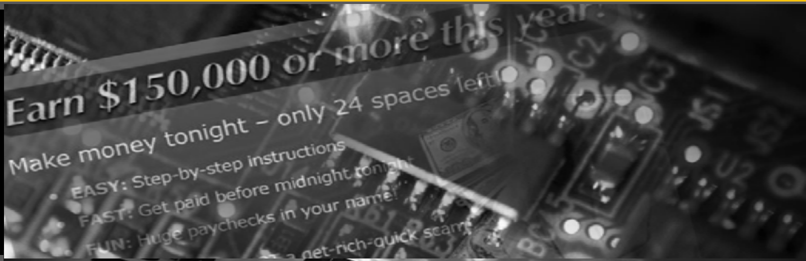
Well
Meaning
Insider

Malicious
Insider

symantec.

Stages Of A Breach

- > Incursion

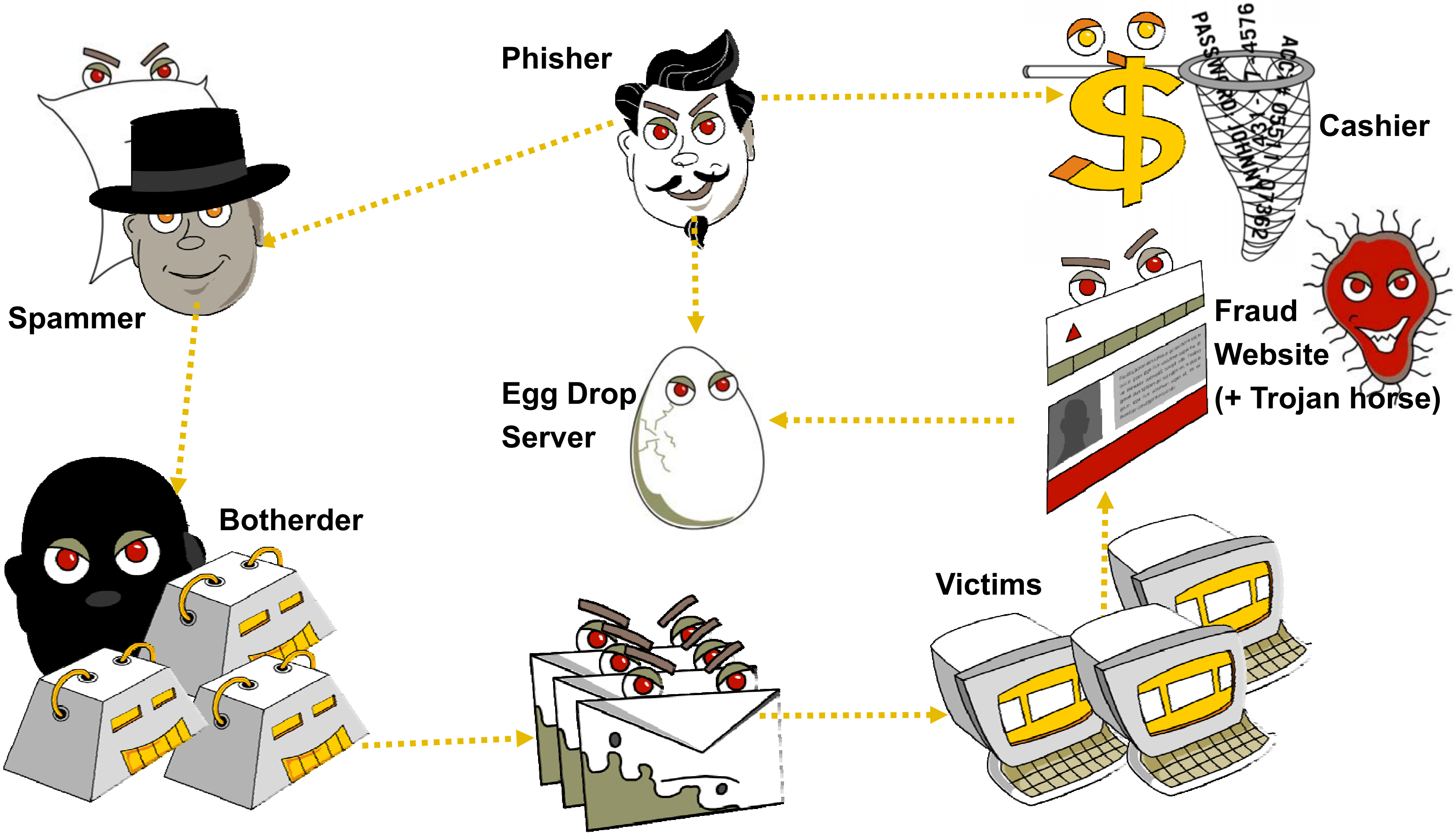

Earn $150,000 or more this year!
Make money tonight – only 24 spaces left!
EASY: Step-by-step instructions
FAST: Get paid before midnight tonight
FUN: Huge paychecks in your name!
get-rich-quick scam

- > Discovery

- > Capture

- > Exfiltration

symantec.



Phisher

Cashier

Spammer

Fraud Website (+ Trojan horse)

Egg Drop Server

Botherder

Victims

Phishing Messages

Security Market Drivers

Capture

285 million records were stolen in 2008, compared to 230 million between 2004 and 2007

Credit card detail accounts for 32% of all goods advertised on underground economy servers

IP theft costs companies $600 million globally

Security Market Drivers

Exfiltration

"Gov't Posts Sensitive List Of US Nuclear Sites" Associated Press

"Goldman May Lose Millions From Ex-Worker's Code Theft"
July 7 (Bloomberg), Goldman Sachs

"2 Men Accused Of Swiping CC Numbers" July 2 (Bloomberg), KPHO.com

"Royal Air Force Embarrassed By Yet Another Sensitive Data Loss"
May 25, UK News

symantec.

Prelude to a

Breach

1

Poorly Protected Infrastructure

Protect The Infrastructure

Secure Endpoints

Protect Email and Web

Defend Critical Internal Servers

Backup and Recover Data

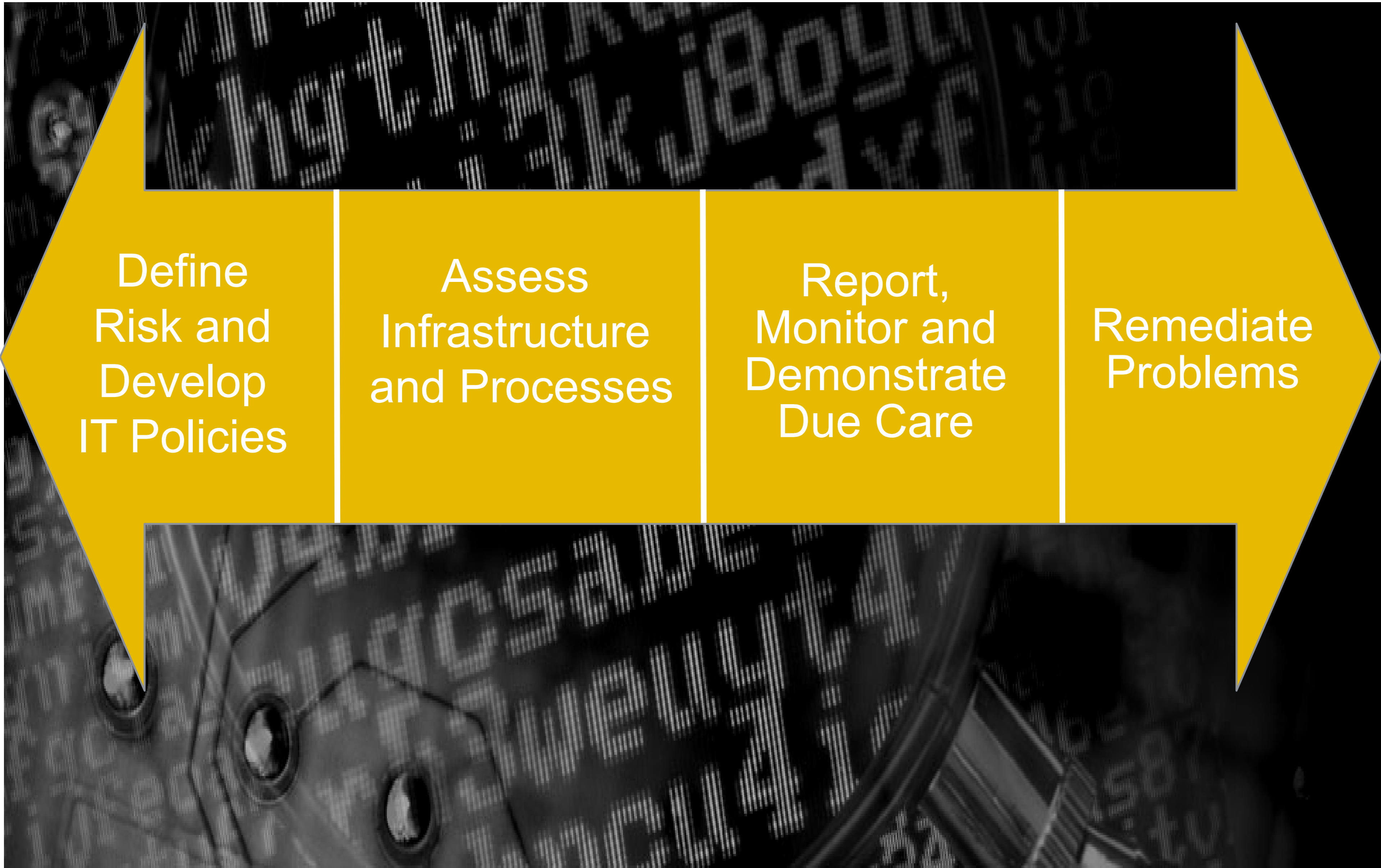
Prelude to a

Breach

2

Lack of IT Policies

Develop and Enforce IT Policies



Define Risk and Develop IT Policies

Assess Infrastructure and Processes

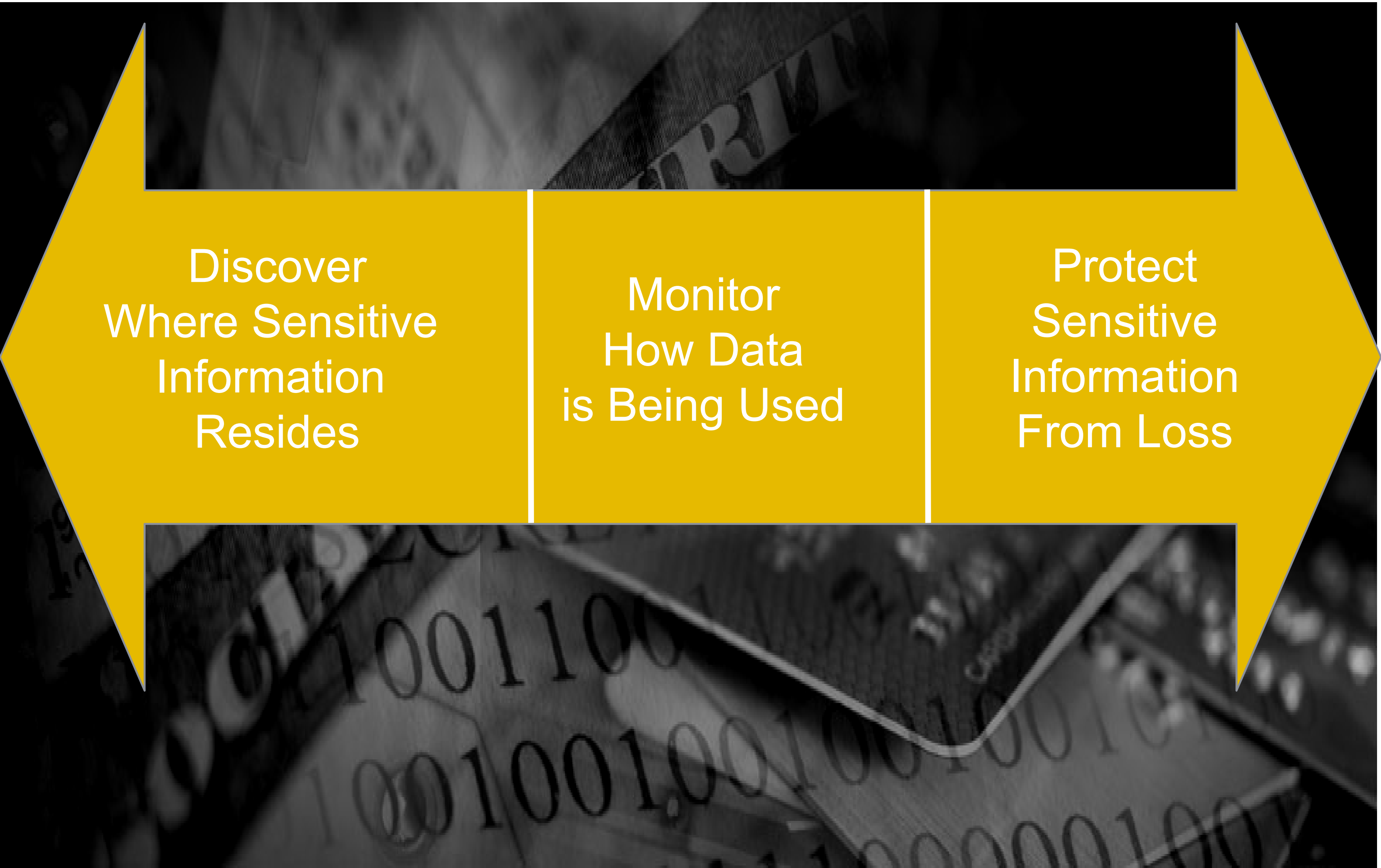
Report, Monitor and Demonstrate Due Care

Remediate Problems

Poorly Protected Information

symantec.

Protect The Information



Discover Where Sensitive Information Resides

Monitor How Data is Being Used

Protect Sensitive Information From Loss

Prelude to a

Breach

4

Poorly Managed Systems

Manage Systems

Implement Secure Operating Environments

Distribute and Enforce Patch Levels

Automate Processes to Streamline Efficiency

Monitor and Report on System Status

Protect the Infrastructure

Develop and Enforce IT Policies

Protect the Information

Manage Systems

symantec.

Thank You

sangam@symantec.com

+91-98451-18021