



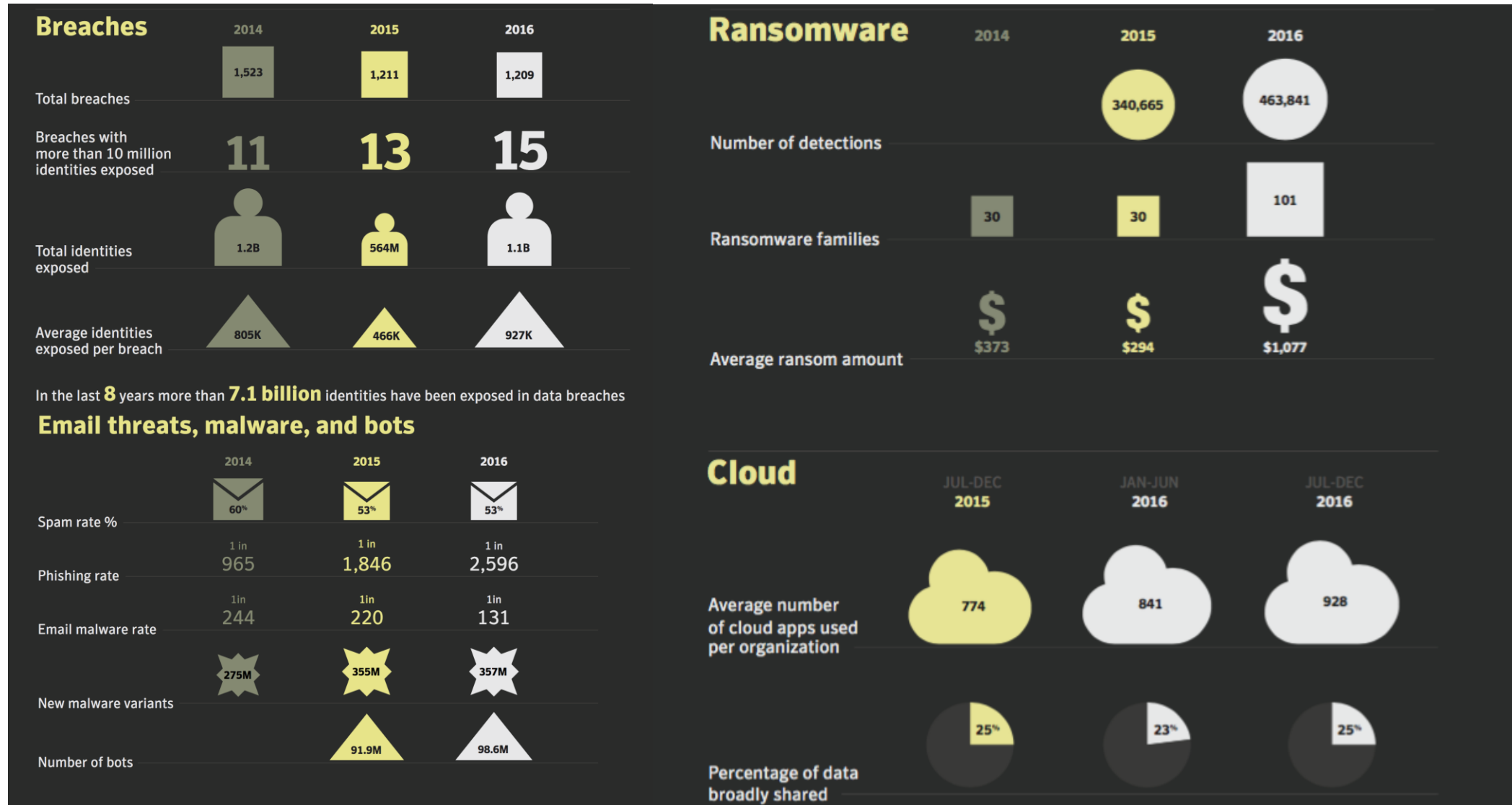
# *Latest Security Trends and Implications For NGO's Information Security Policies*

# Agenda

- Trend of IT & Cyber Crime
- Cisco Practices
- Suggestions
- Q&A



# Cyber Crime Trend



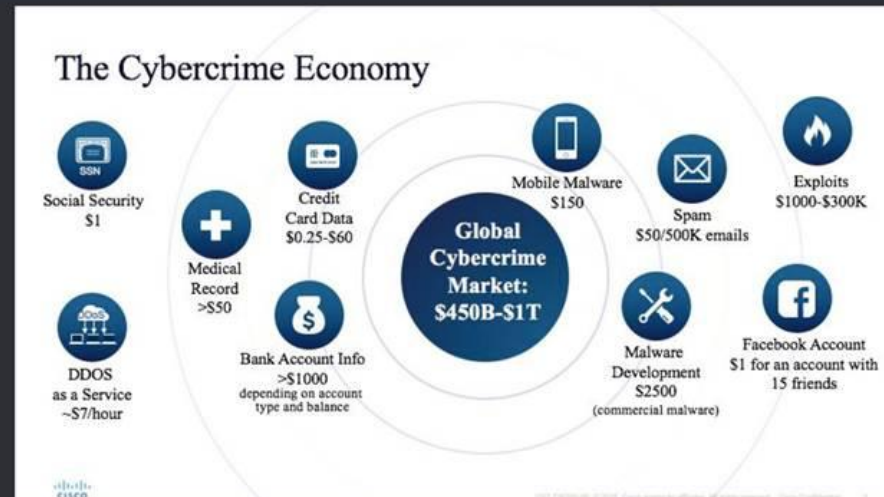


翡翠台

黑服務	價錢(美元)
盜取銀行帳戶資料	>\$1000 (視乎帳戶類型與存款)
盜取社交媒體帳戶	\$1 (有15個朋友的帳戶)
盜取醫療記錄	>\$50
盜取信用卡資料	\$0.25-\$60
發放垃圾郵件	\$50 (發放50萬封垃圾郵件)

**全球網絡罪案潛在市場總值：4,500億至10,000億美元**

資料來源：思科香港 (2015-2016年數據)



- We know what hackers are doing
- We have the most comprehensive threat intelligence on latest threats around the world

TALOS

# The Evolution of the Cyber Criminal

Now a sophisticated business focused on ROI

## Old School Hackers



Cyber-punks/Hackers



Unsophisticated



Individual's Data



Notoriety/Political



Opportunistic



Nation State

## New School Cybercriminal



Professional  
organized crime



Strategic Assets



Multi-Billion \$\$  
Business



Targeted/ROI



**Sophisticated** Supply  
Chains



Nation State

# WannaCry Outbreak



230,000

150

72

FedEx®

Telefonica

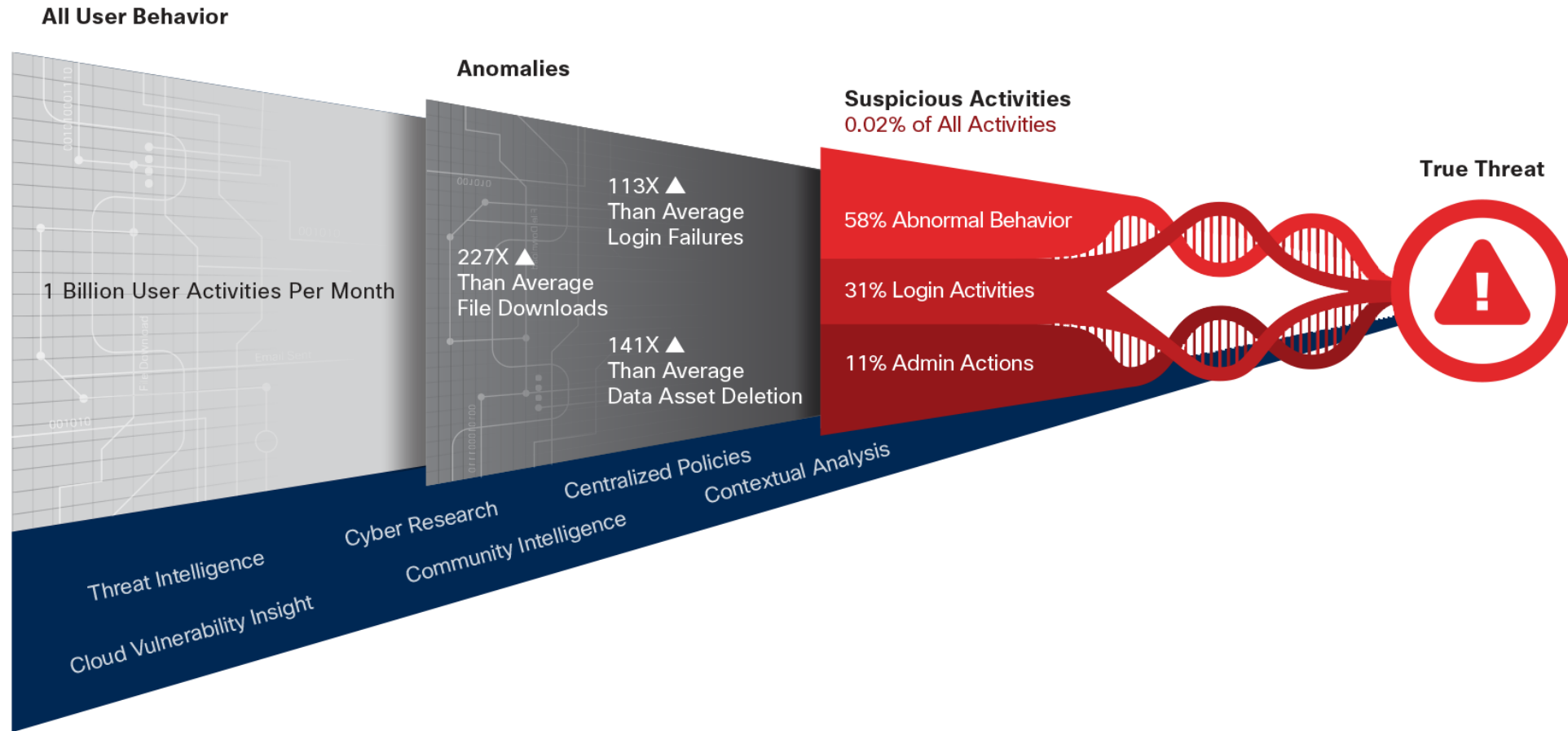
NHS



We're lucky, the damage could have been much more severe



# Cisco Practices –Identifying User Behavior Patterns with Automation



# How do we prioritize?



## Advanced Threats

- Spear Phishing and Trojans
- Watering hole attacks
- Social networking attacks
- Nation state attacks



## Evolving Solutions

- Expanded data collection
  - Netflow, IP Attribution, DNS...
- Big data analysis and playbooks
- Rapid containment
  - DNS/RPZ, Quarantine, On-line host forensics
- Threat/Situational awareness (TALOS)



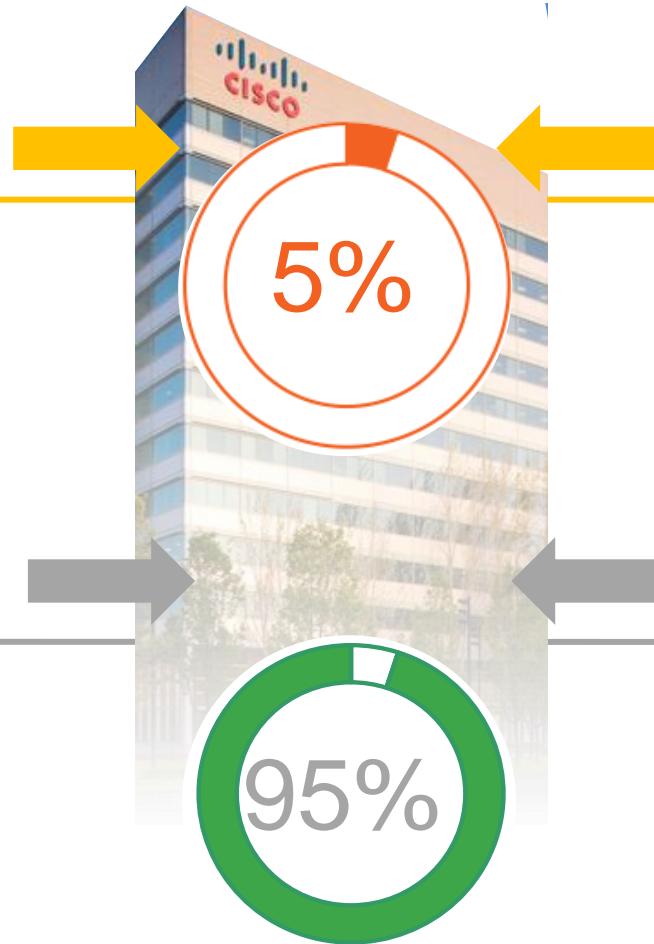
## Security Challenges

- Manager/Unmanaged desktops
- Spam/Malware
- DDoS
- Compromised hosts remotely controlled
- Rapidly changing environment



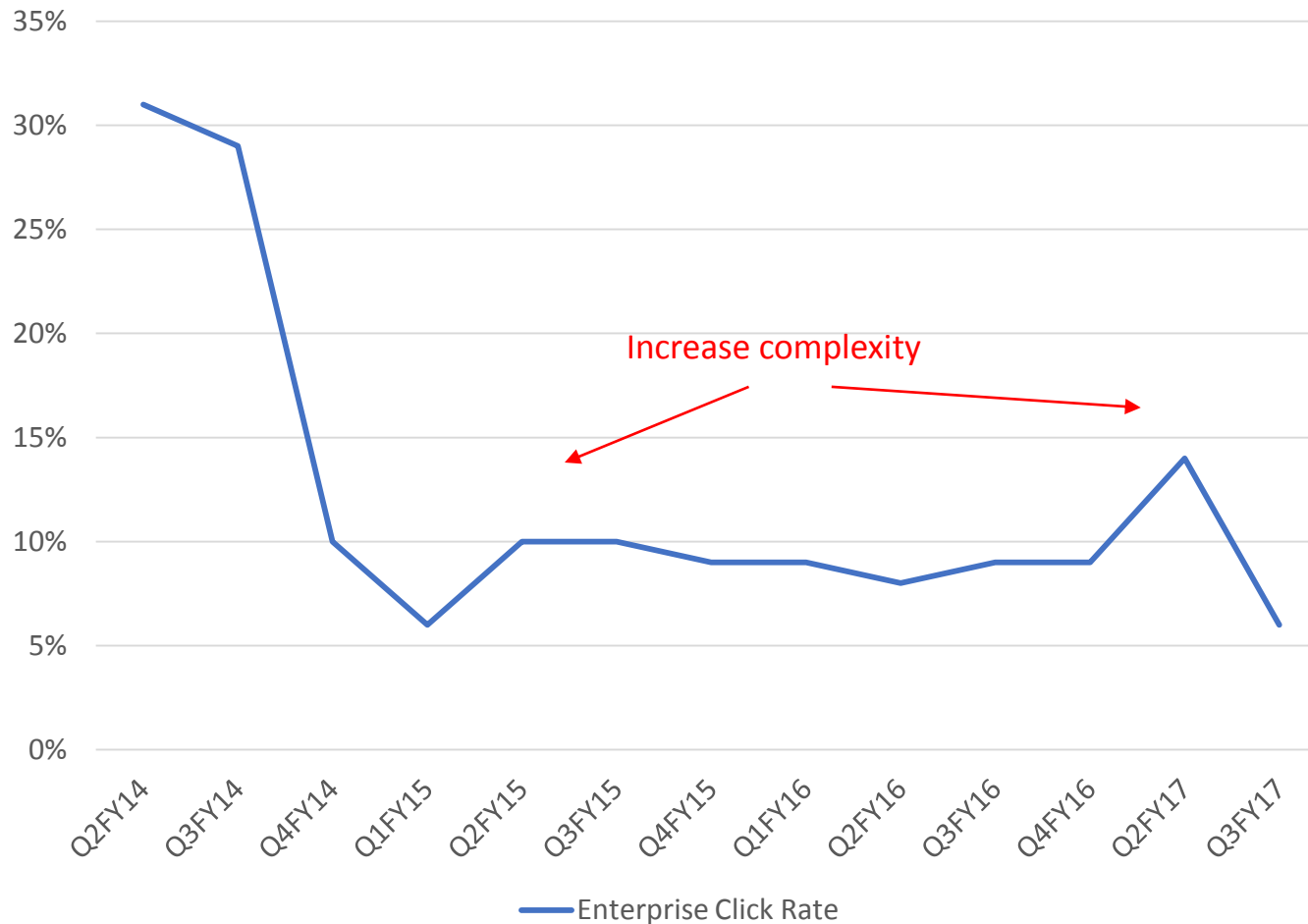
## Foundational Solutions

- Anti-virus/Anti-malware
- Firewalls (FirePower)
- IDS/IPS
- Web Security Appliance/ESA
- Network segmentation
- Log capture/analysis
- Incident response team





# Cisco Practices -- Anti-Phishing




**Compared to 30% industry average click rate:**

- Cisco has improved dramatically since phishing program started
- Complexity of test phish is increasing, expect temporary rise in click rates
- Shifting focus to educate users who repeatedly click phish

# How will this impact NGO?

Threat

Action



Adaptive Security	<ul style="list-style-type: none"><li>• Cloud Security</li><li>• Defense-in-depth</li><li>• Architecture Redesign</li></ul>
Security Vigilant	<ul style="list-style-type: none"><li>• Anti-phishing</li><li>• Training &amp; Awareness</li><li>• Proper Monitoring &amp; Responding</li></ul>
Data Security	<ul style="list-style-type: none"><li>• Proper Social Media Usage</li><li>• Customer Data Protection</li><li>• Data Intelligence &amp; Analytic</li></ul>

# Suggestions – Drill Down

- Situational Awareness – Understand your risk
- Defense in Depth
  - Parameter Security – Firewall, Email Sec, Web Sec, IDS/IPS
  - Endpoint Security – Patch Mgmt, Anti Virus /Malware, Network Access Control
  - DC Security – Server Hardening, Change Mgmt, Vulnerability mgmt
  - App Security – Vulnerability Mgmt, Auth-C/Z
  - People – Awareness/Education, anti-phishing
- Cloud Security
  - Cloud Access Security Brokers (CASB)
  - Cloud Security Review Process, Cloud Tenant Security
- Monitoring and Responding
  - Activity monitoring, Anomaly detection, Data intelligence Analytics
- Data = Money
  - Customer Data Protection / Data Loss Prevention
  - Data backup/restore/**retention**



**Find Right Help**



# Q&A