sibos TORONTO 16 - 19 Oct 2017

SWIFT INSTITUTE

Forces shaping the cyber threat landscape

sibos TORONTO
16 - 19 Oct 2017

SWIFT INSTITUTE

William A. Carter

Deputy Director
CSIS Technology Policy Program

1. Attack Surface

- Mobile banking
- Internet of Things
- Changing geography of cyberspace

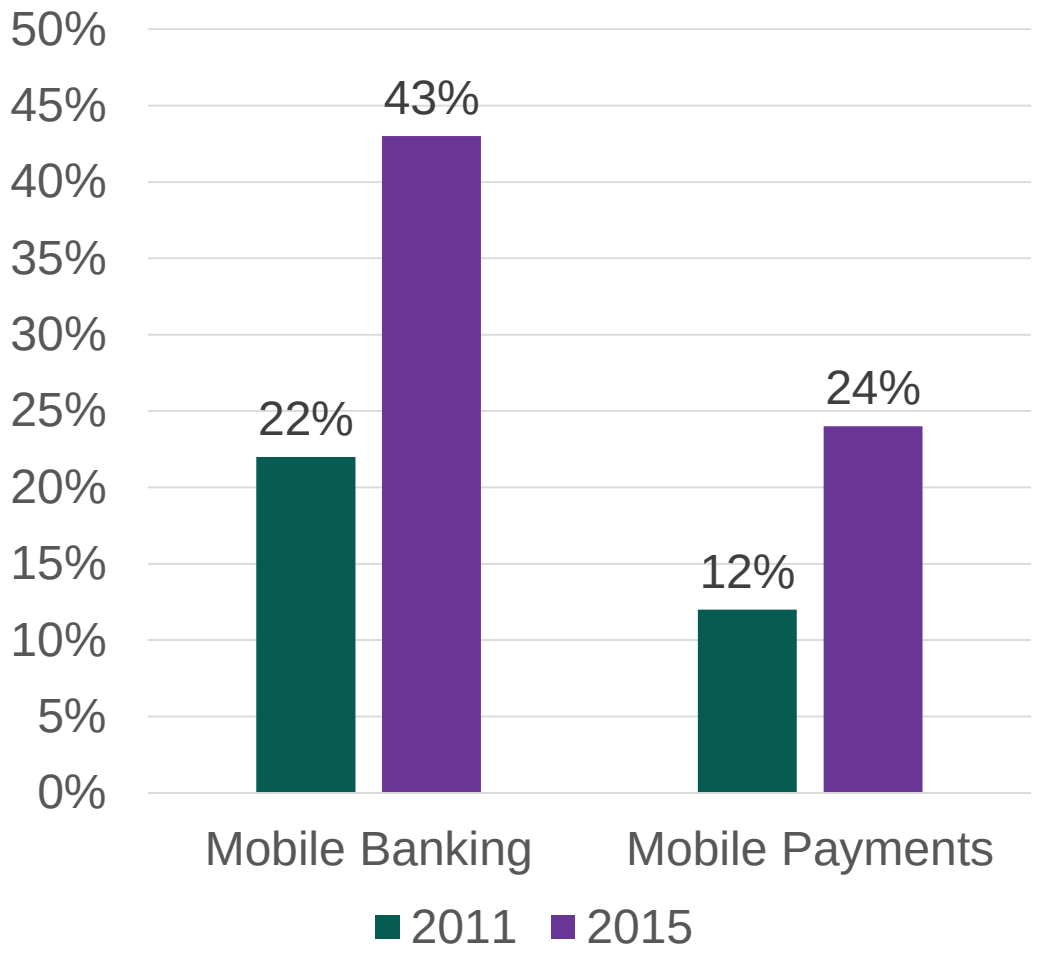
2. Attacker Incentives

- “Nation-states are robbing banks.”
- Criminal groups more sophisticated, organized
- Law enforcement capacity

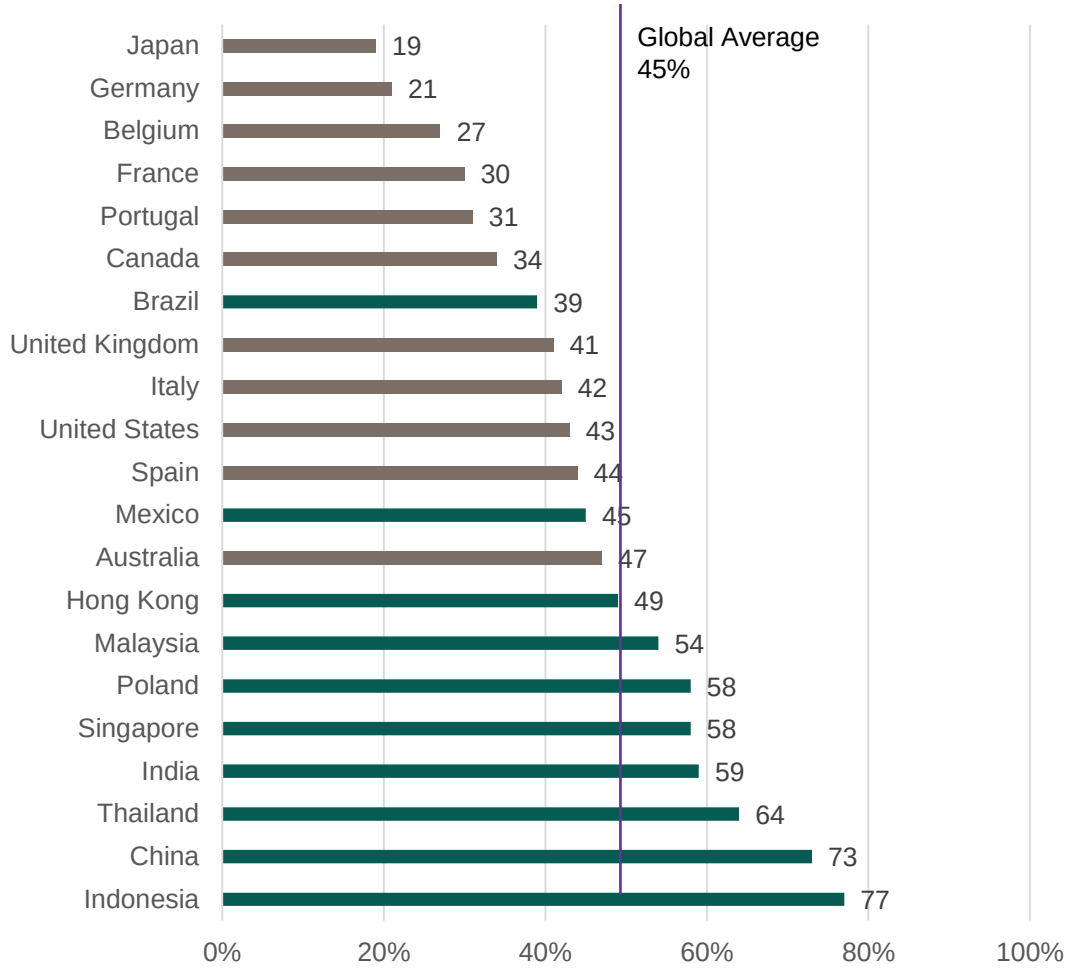
3. New Defenses

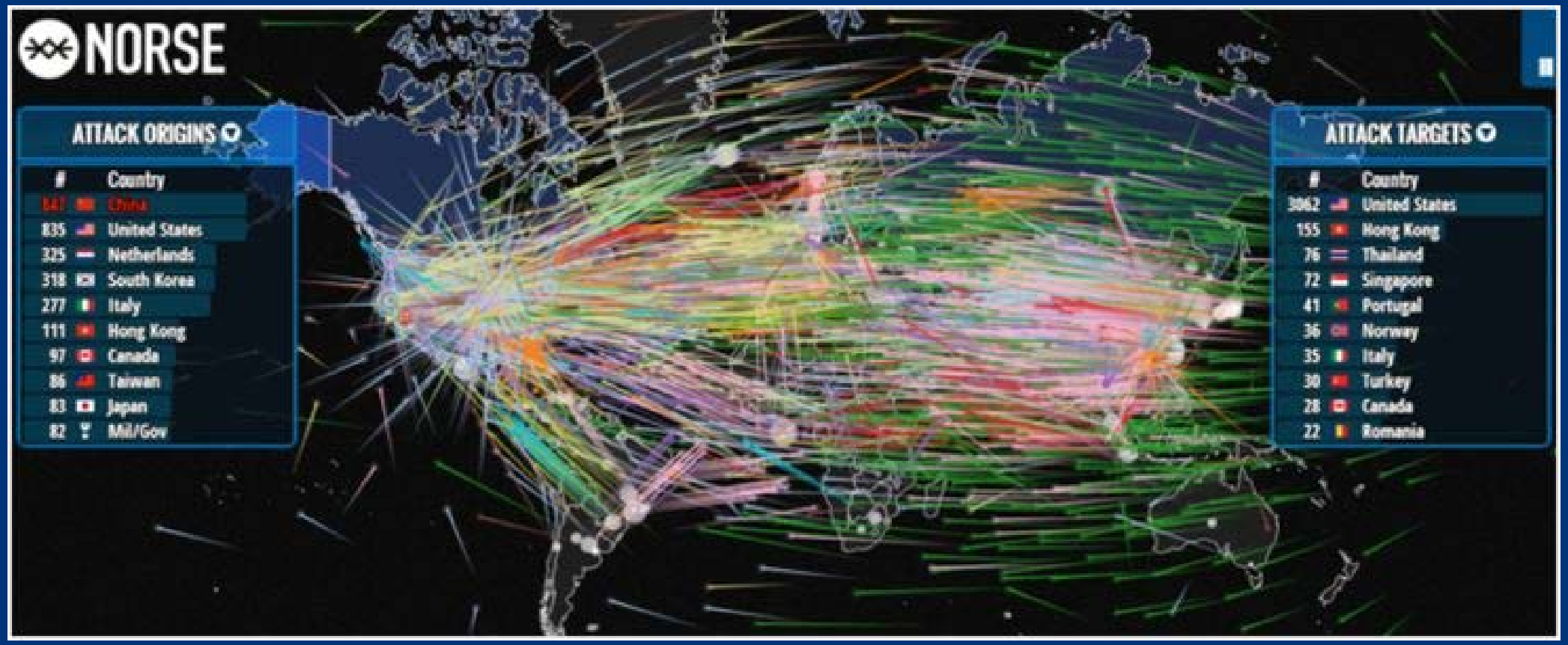
- DDoS Mitigation
- Cyber hygiene training
- Behavioral analytics
- Multi-factor authentication

Growth of Mobile Banking and Mobile Payments in the US



Mobile Banking Penetration Around the World




NORSE
ATTACK ORIGINS
Country
847 China
835 United States
325 Netherlands
318 South Korea
277 Italy
111 Hong Kong
97 Canada
86 Taiwan
83 Japan
82 Mil/Gov
ATTACK TARGETS
Country
3062 United States
155 Hong Kong
76 Thailand
72 Singapore
41 Portugal
36 Norway
35 Italy
30 Turkey
28 Canada
22 Romania


Novosibirsk
Baikal
Tynda
Irkutsk
Chita
Astana
Semey
(Semipalatinsk)
KAZAKHSTAN
Ulaanbaatar
MONGOLIA
Hailar
Khabarovsk
Burqin
Harbin
Aral Sea
Lake Balkhash
Almaty
Ürümqi
Vladivostok
Sapporo
Bishkek
KYRGYZSTAN
Tashkent
Shenyang
Beijing
NORTH KOREA
Sea of Japan
Demarcation Line
Kashi
Yinchuan
Tianjin
Pyongyang
Seoul
SOUTH KOREA
JAPAN
TAJIKISTAN
Dushanbe
Indian claim
1972 Line of Control
Golmud
Lanzhou
Yellow Sea
Osaka
Tokyo
Kabul
Herāt
Line of Actual Control
CHINA
Xi'an
AFGHANISTAN
Islamabad
Nanjing
Shanghai
Lhasa
East China Sea
PAKISTAN
New Delhi
NEPAL
Kathmandu
BHUTAN
Thimphu
Chengdu
Wuhan
Jaipur
Lucknow
Fuzhou
Taipei
Okinawa
Udaipur
Karāchi
Kunming
Dhaka
Tropic of Cancer
Guangzhou
INDIA
Kolkata
BANGLADESH
Macau S.A.R.
Hong Kong Special Administrative Region
Taiwan
Mandalay
BURMA
LAOS
Hanoi
Vientiane
Hainan Dao
Mumbai
Hyderābād
Vishākhapatnam
Paracel Islands
Arabian Sea
Bay of Bengal
Rangoon
THAILAND
Bangkok
Da Nang
VIETNAM
Manila
Philippine Sea
Northern Mariana Islands (U.S.)
Chennai
Andaman Islands (INDIA)
Andaman Sea
CAMB.
South China Sea
PHILIPPINES
Guam (U.S.)
Lakshadweep (INDIA)
Phnom Penh
Ho Chi Minh City
Spratly Islands
Cebu
FEDERATED STATES OF MICRONESIA
Cochin
SRI LANKA
Nicobar Islands (INDIA)
Phuket
Davao
Koror
PALAU
Colombo
Bandar Seri Begawan
BRUNEI
Banda Aceh
Kuala Lumpur
MALAYSIA
Male
MALDIVES
Medan
Singapore
SINGAPORE
Borneo
Manado
Equator
Equator
Padang
Samarinda
Sorong
British Indian Ocean Territory (U.K.)
Palembang
I N D O N E S I A
New Guinea
PAPUA NEW GUINEA
Jakarta
Makassar
Diego Garcia
Surabaya
Dili
EAST TIMOR
Port Moresby
Kupang
Indian Ocean
Christmas Island

ICT4C

Bank Fraud Thriving in the Developing World

- Infrastructure development and proliferation of mobile is fueling cybercrime in Africa and Latin America
- Africa, in particular, is seeing a significant uptick in cybercrime
  - Governance challenges create haven for criminals
  - EU law enforcement report European criminal groups relocating to Africa as intra-EU law enforcement cooperation improves
- Brazil – fraud capital of the world?
  - 57% of all banking transactions in Brazil are digital
  - 50% of Brazilians have been victims of banking fraud in the last five years
  - Brazilian fraudsters are starting to attack outside Brazil

How the Carbanak cybergang stole $1bn

A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected
in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

Hacker

Cash transfer systems

Admin

Rec

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

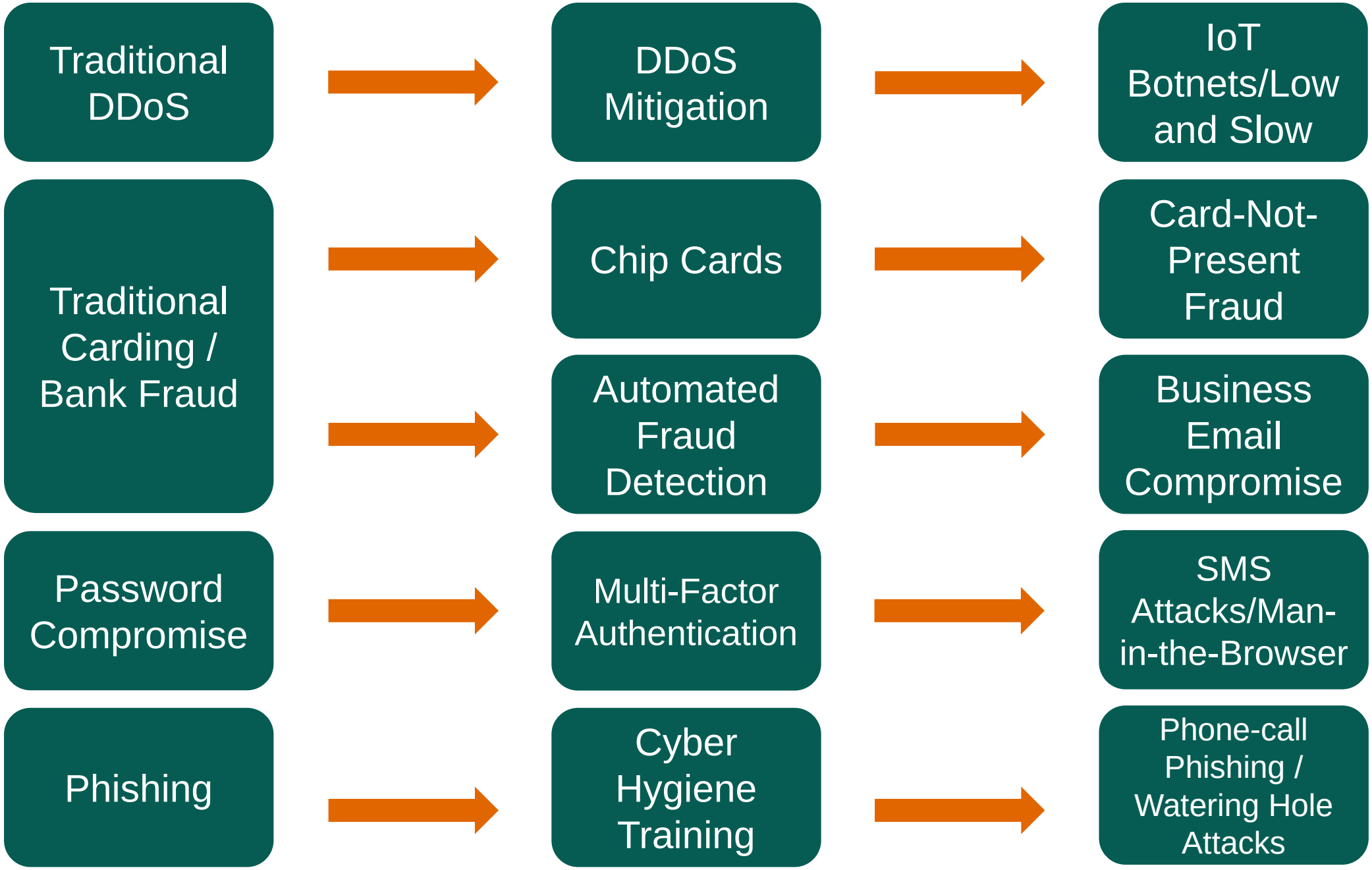
Controlling ATMs
Orders to dispense cash at a pre-determined time

GREAT KASPERSKY lab

Law Enforcement Struggling to Keep Up

Four challenges continue to plague cyber law enforcement:

1. Lack of resources
   - Technical specialists, qualified analysts, compute resources, funding, digital evidence training for rank-and-file police
2. Lack of clear authorities to prosecute cybercrime
   - Many countries still have no official cybercrime laws, or have different definitions of cybercrime
3. Procedural hurdles
   - Jurisdiction, chain of evidence, key disclosure, explaining to juries
4. Cross-border challenges
   - Inconsistent laws governing cybercrime around the world
   - Inadequate evidence sharing and extradition mechanisms
   - Lack of capacity in many countries to investigate cybercrimes
   - Some countries offer “safe havens” for cybercriminals


Traditional DDoS
DDoS Mitigation
IoT Botnets/Low and Slow
Traditional Carding / Bank Fraud
Chip Cards
Card-Not-Present Fraud
Automated Fraud Detection
Business Email Compromise
Password Compromise
Multi-Factor Authentication
SMS Attacks/Man-in-the-Browser
Phishing
Cyber Hygiene Training
Phone-call Phishing / Watering Hole Attacks

Conclusion: More Threats, More Complexity, More Sophistication

Consumer fraud: New defenses and mobile banking are transforming the landscape

- As consumer bank fraud becomes harder, business customers are being targeted
- Mobile malware is the new frontier of consumer fraud
- ICT4C: Financial inclusion is creating new threats in the developing world

Targeted Attacks on Bank Networks: What is Changing?

- Attackers are becoming more sophisticated, persistent
- Law enforcement still struggling to keep up
- Banks in Asia are top targets
- Vectors of compromise – new twists on old themes
- Hybrid attacks the new normal

Two Interesting Questions from the Research

Is Hacktivism Dead, or Will it Come Back with a Vengeance?

Hacktivist activity has plummeted off the radar of many financial institutions. Once considered a top threat, most financial institutions and law enforcement officials no longer view it as a serious threat at all.
Will it come back?

1. *Hacktivism is dead:* After LulzSec takedown, many skilled hackers realized that hacktivism draws law enforcement attention but is not impactful.
    - Old-school black hats used to engage in hacktivism, but the black hat space is increasingly financially-motivated. Old-school black hats have gone legit and will not risk their legitimate businesses for hacktivism, while today's criminal black hats won't waste their time or risk law enforcement attention on their money-making criminal activities. The remaining hacktivists are glorified script-kiddies that don't pose a threat.

2. *A hacktivist wave is just around the corner*: While hacktivism has been dormant in recent years, the conditions are ripe for a resurgence.
    - Hacktivism against banks has waned because hating the banks isn't sexy anymore. Occupy failed, Anonymous disintegrated, and fighting the power got old. But with the rise of the Trump Era, Brexit, and a growing global focus on corruption and cronyism, banks are about to step back into the limelight in the worst way.

Why Aren’t Small and Medium-Sized FIs Getting Swamped?

Big IFCs invest billions in cybersecurity, but still get hit with hundreds of millions of dollars a year of losses due to cyberattacks. With millions of dollars in their accounts, small dedicated cybersecurity budgets, few to zero cyber professionals on staff, often poor patching practices, and off-the-shelf infrastructure often decades old, why are small and medium banks, credit unions, and insurance companies not getting robbed blind?

1. *Back end service providers are secretly great at cybersecurity:* Back-end service providers’ (in the US we have the big 4 – FIS, Fiserv, D+H, and Jack Henry) customers do seem not to be hurting from cybercrime the way that they should be. Maybe they’re secretly really good at cybersecurity?

2. *There are no mid-market cybercriminals*: The cybercrime economy is bifurcated. There are highly sophisticated, organized criminal organizations that target big IFCs for enormous payouts and low-level criminals that don’t even both to go after FIs.

3. *Hacking local banks isn’t cool*: The local credit union isn’t exactly a fortress. Your grandma banks there. It doesn’t take any skillz to get in, so why would anyone be impressed that you did it? Many top hackers are in it for the reputation as much as the money, so they focus on big banks.

Questions

sibos TORONTO 16 - 19 Oct 2017

SWIFT INSTITUTE

Research paper can be downloaded from:

www.swiftinstitute.org