

Forces Shaping the Cyber Threat Landscape for Financial Institutions

William A. Carter
Associate Director
CSIS Technology Policy Program

Putting the Problem in Perspective

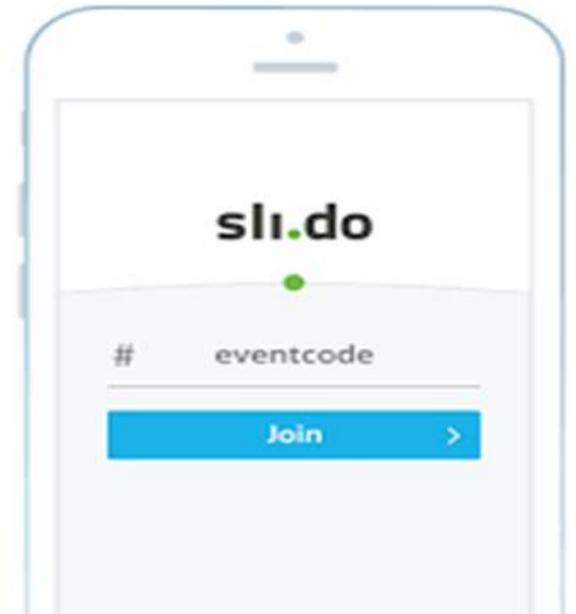
What Sector is the Top Target of Cyber Attacks?

1. Healthcare
2. Financial Services
3. Government
4. Retail
5. Energy
6. Utilities
7. Telecom
8. IT
9. Manufacturing
10. Materials



What Cyber Threats Worry You the Most?

1. Extortion (DDoS, Ransomware)
2. Data theft (customer PII, IP, communications, deal info)
3. Fraud (Carding, Account Fraud, Illicit Transfers)
4. Destructive malware (wiper variants, ransomware)
5. Data manipulation



What Forces Shape the Threat Landscape?

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



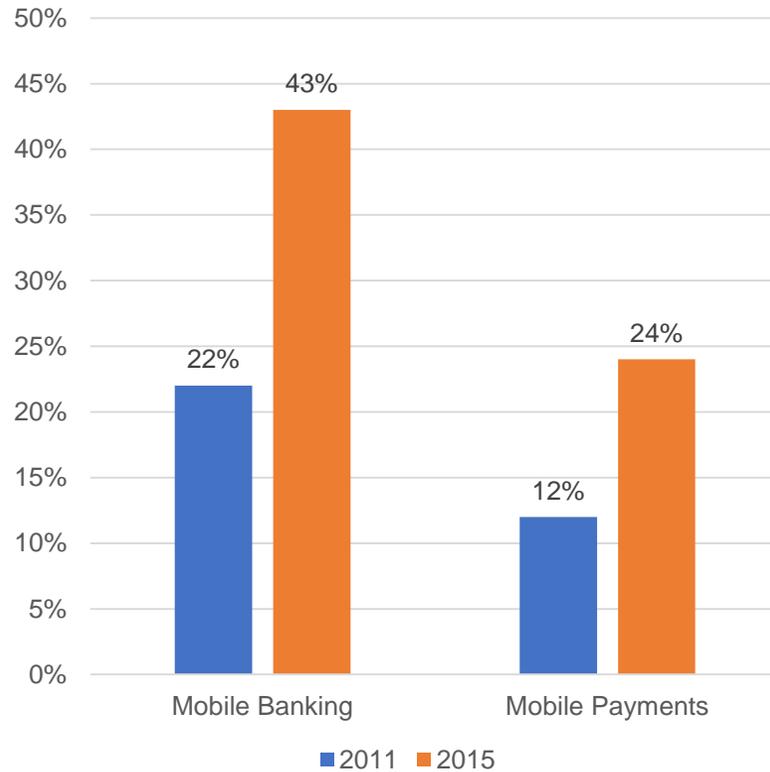
- DDoS Mitigation
- Cyber hygiene training
- Behavioral analytics
- Multi-factor authentication

“Defenders Have a Narrow View of What Counts as a Computer”

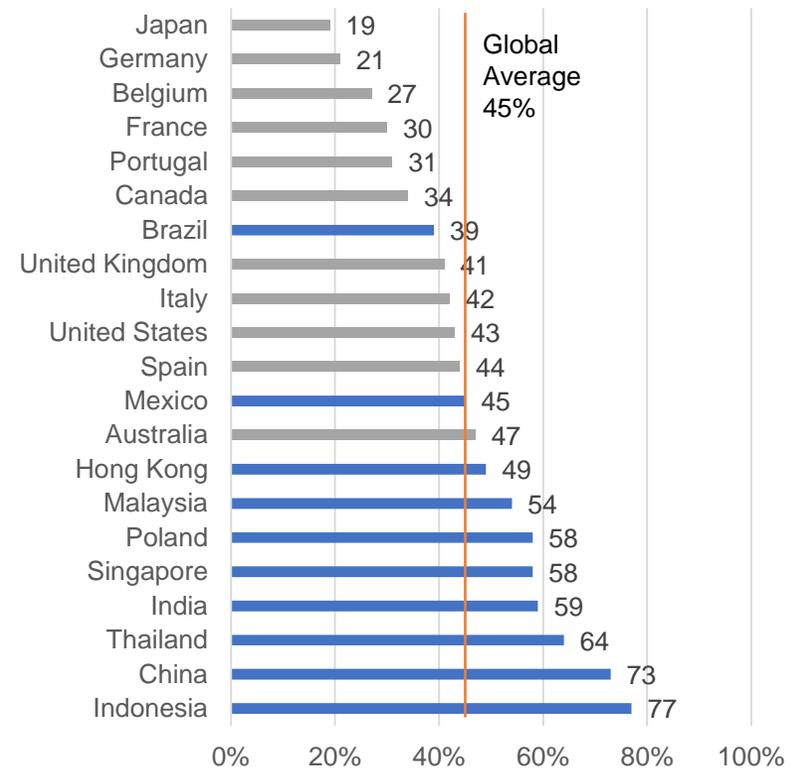


Mobile Banking is Transforming the Landscape

Growth of Mobile Banking and Mobile Payments in the US



Mobile Banking Penetration Around the World



The Geography of Cybercrime is Changing



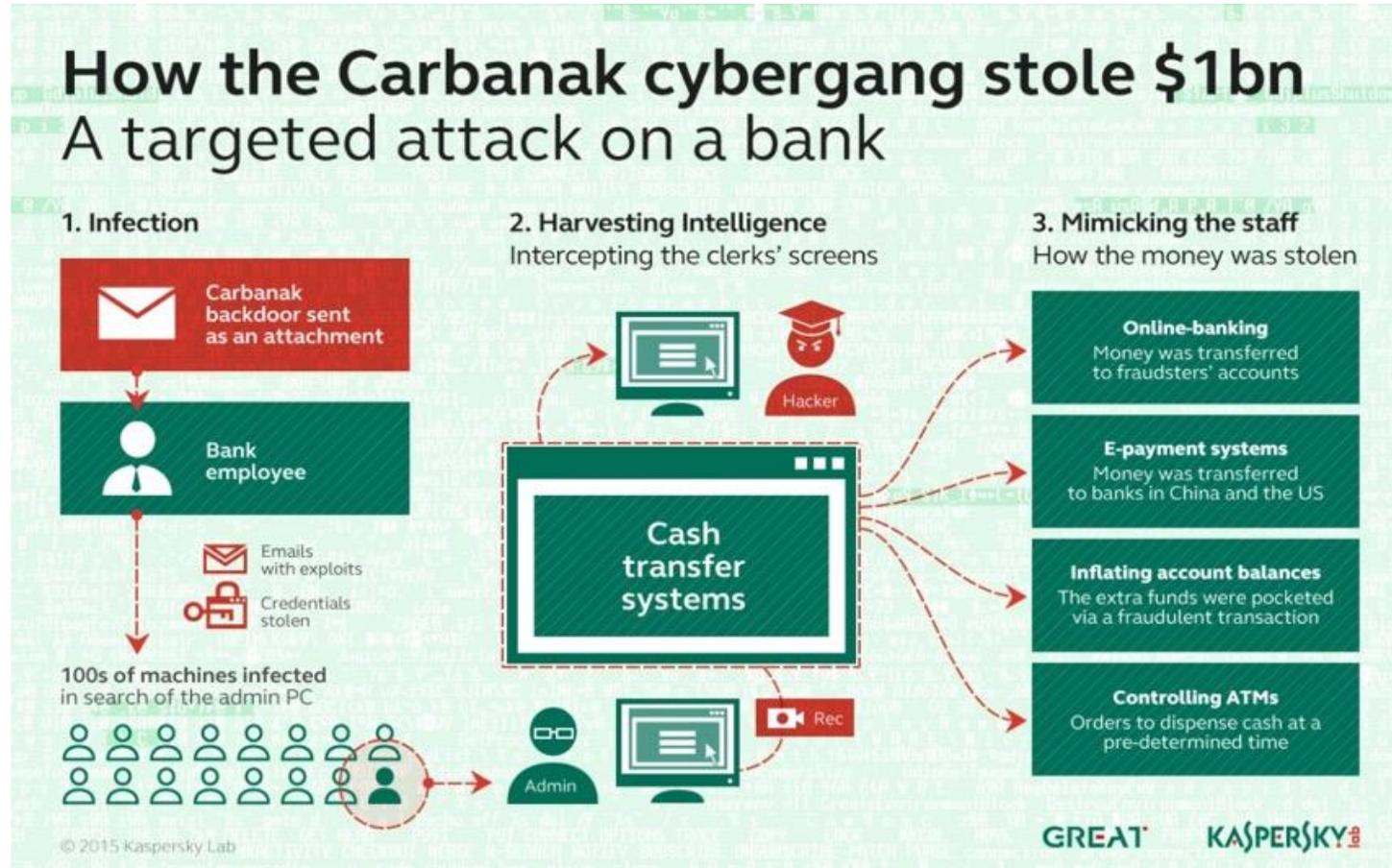
ICT4C – Bank Fraud Thriving in the Developing World

- 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

“Nation states are robbing banks”



Criminal Groups are Increasingly Sophisticated, Organized

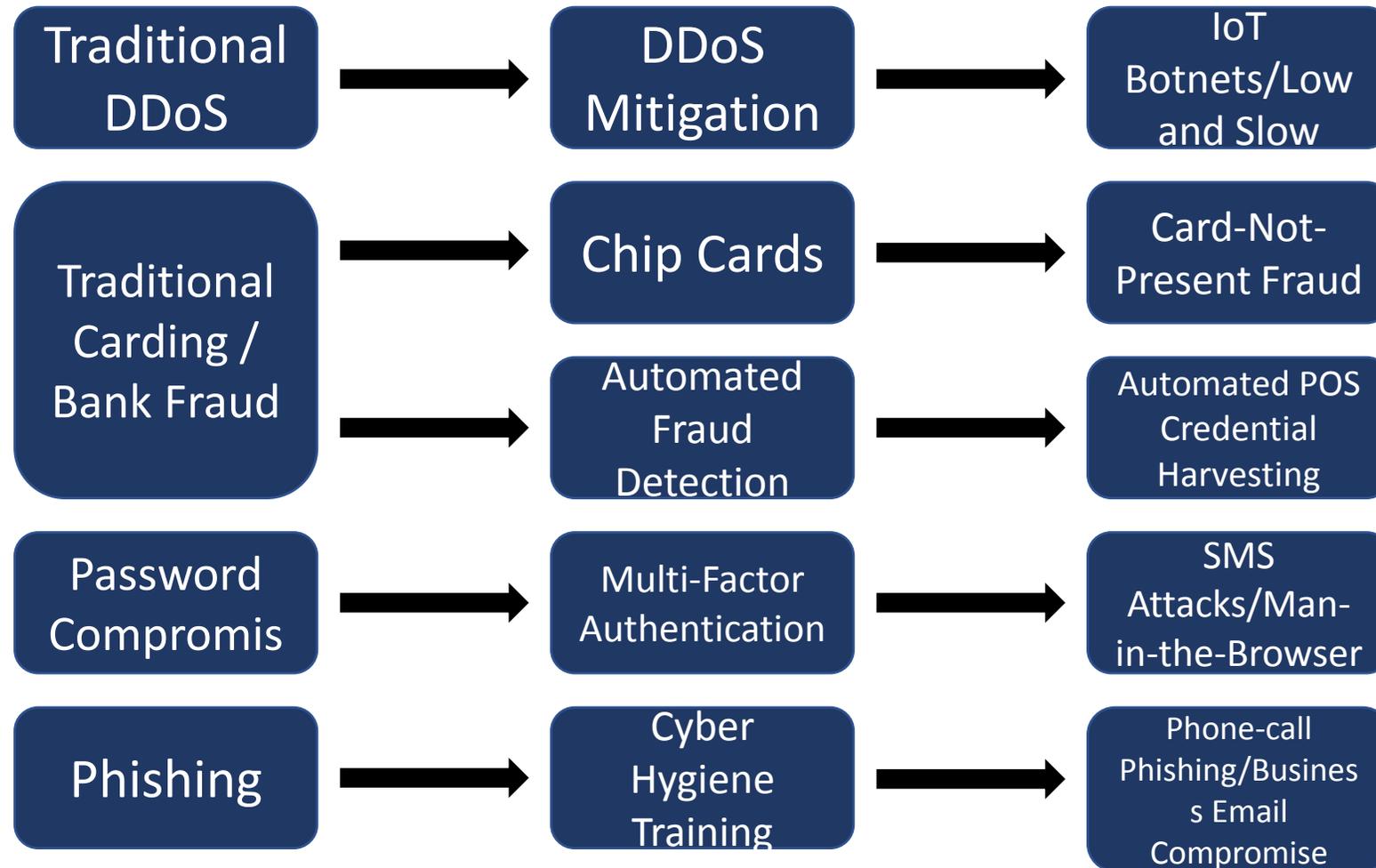


Law Enforcement Struggling to Keep Up

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

Attackers Adapt to Defenses, to a Point



Conclusion: More Threats, More Complexity, More Sophistication

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

- New defenses are transforming consumer fraud and carding
- As consumer bank fraud becomes harder, business customers are being targeted
- Mobile malware is the new frontier of consumer bank 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
- Vectors of compromise – new twists on old themes
- Attacks methods are changing

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 bother 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.