Forces Shaping the Next Generation of Cyber Threats to Financial Institutions

William A. Carter
Associate Director
CSIS Technology Policy Program

Cybercrime is a booming industry

- One study by Verizon recorded 65 ***thousand*** data breaches in 2015
- An estimated 320 – 430 ***million*** pieces of new malware were created in 2015
- The global cybersecurity market was estimated at **$81.6bn** in 2017, but a 2014 CSIS study estimated the cost of cybercrime at more than **$400bn** per year
- According to a 2013 UN study, as much as **17%** of the online population are victims of digital theft every year, whereas just 5% of the population are victims of physical crime

“Why do you rob banks? Because that’s where the money is!”

- Financial institutions are the #1 targets of cyber criminals
- According to one study, 40% of successful data exfiltrations target financial institutions
- The average cost of data breaches to financial institutions is estimated at $221 for each individual customer record lost!
- Fraud prevention remains difficult. In one study of illicit online fund transfers:
  - 22% of transfers were blocked
  - 10% of illegally transferred funds were recovered
  - 68% were declared unrecoverable

Forces Shaping the Threat Landscape

What Forces Shape the Threat Landscape?

1. Attack Surface

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

2. Attacker Incentives

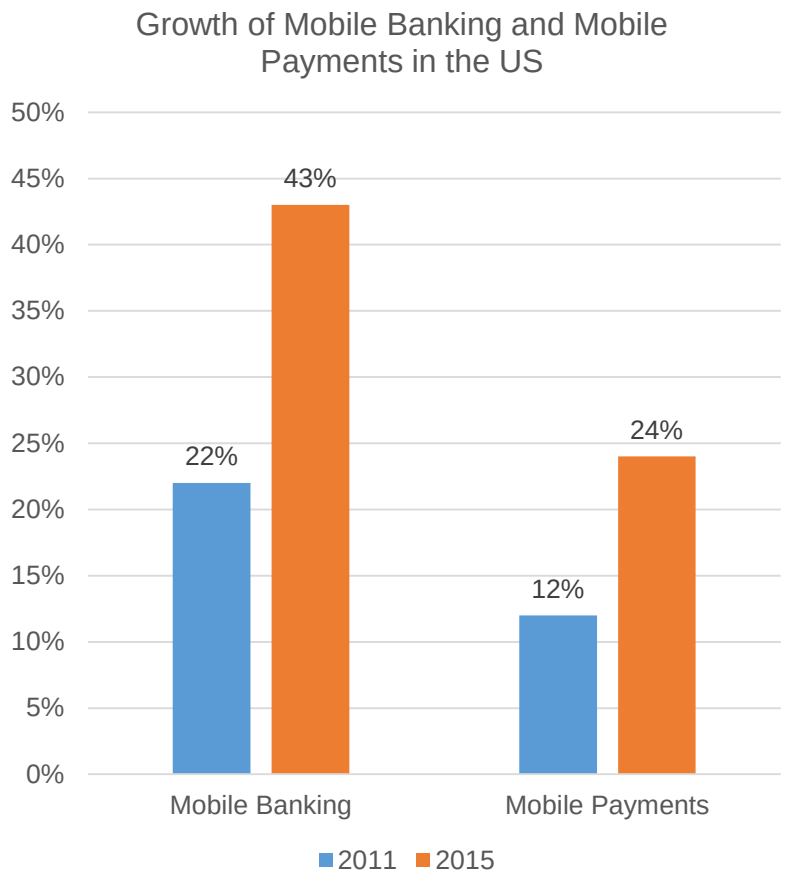
- “Nation-states are robbing banks.”
- Criminal groups more sophisticated, organized
- Law enforcement capacity

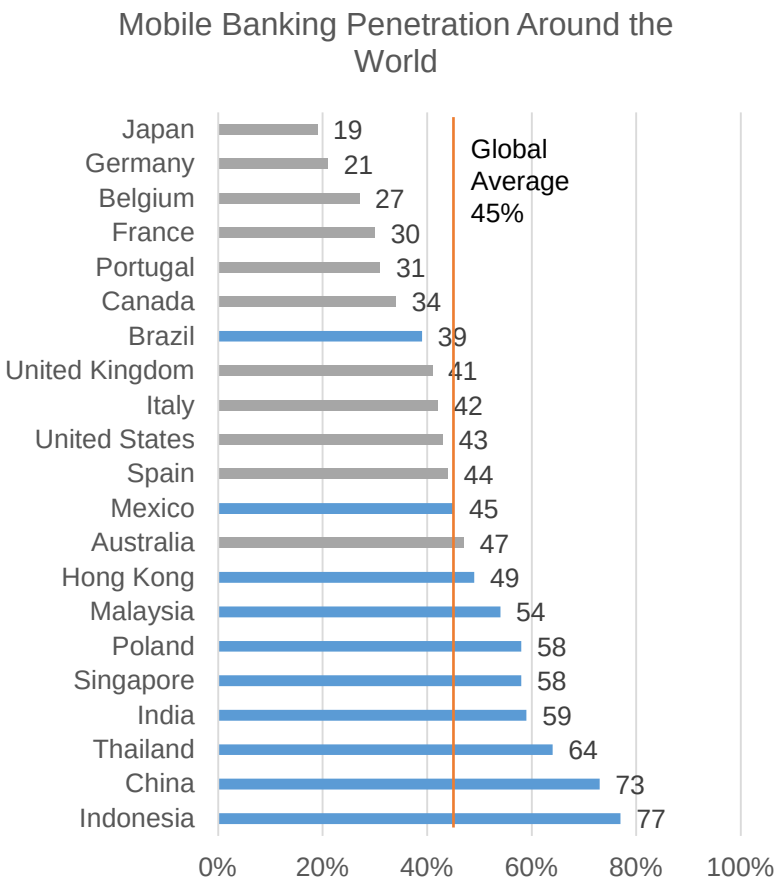
3. New Defenses

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

1. Attack Surface

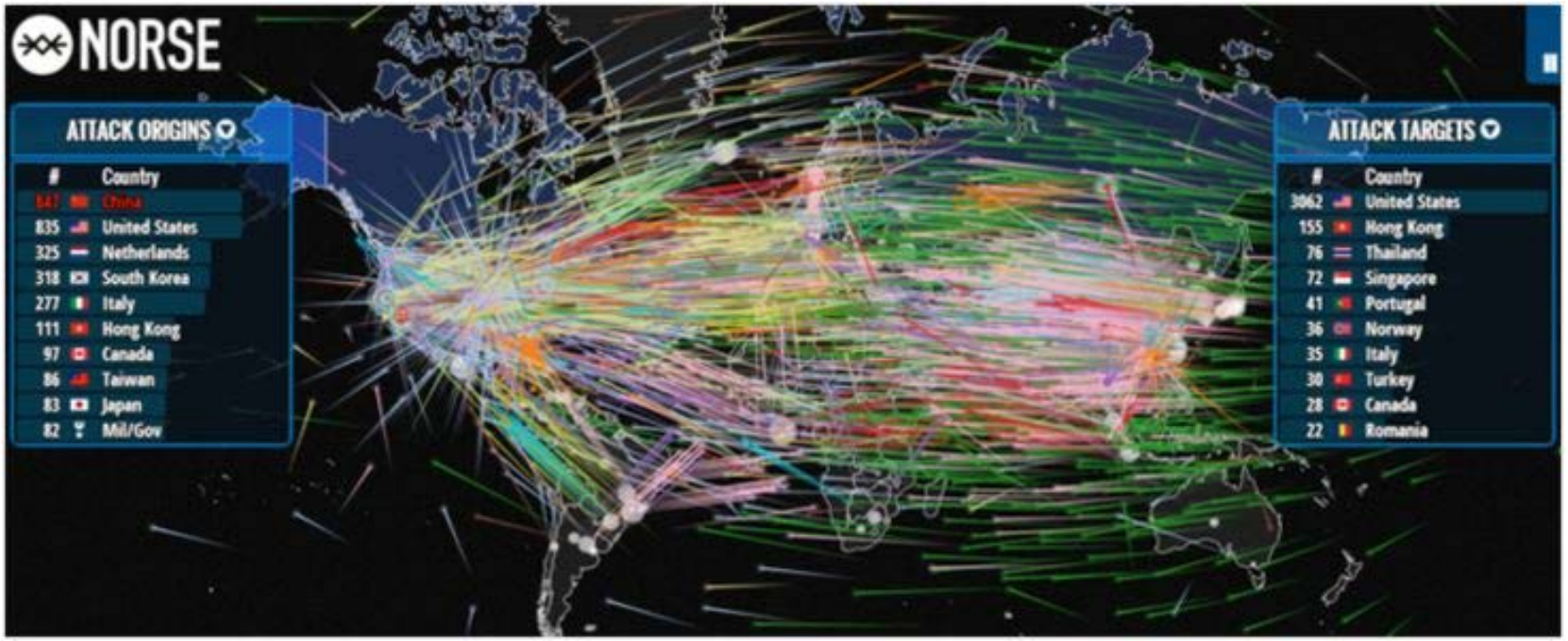
Mobile Banking is Transforming the Landscape





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

The Geography of Cybercrime is Changing



Asian Banks are in the Spotlight

Asian banks are viewed as prime targets with weak security and high value:

- Regulatory vacuum/inconsistency
- Large customer bases
- Growth over security
- Poor AML practices
- Criminal translation services
- Will regulatory/legislative pressure on cyber decrease opportunities?

Asian cybercriminals are also increasingly targeting banks outside of Asia

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
  - Poor governance creates 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?
  - 45% of all banking transactions in Brazil are digital
  - 50% of Brazilians have been victims of banking fraud in the last five years
  - Boleto campaign – 500,000 fraudulent transactions, 30 banks
  - Brazilian fraudsters are starting to attack outside Brazil
    - e.g. UK bank breach – 9,000 user accounts robbed in 24 hours

2. Attacker Incentives

“Nation states are robbing banks”

3 key trends to watch:

1. Nation-states engaging in financially-motivated cybercrime targeting banks
2. Nation-states hacking financial institutions for political/strategic leverage
3. Nation-state-linked criminal groups launching sophisticated criminal campaigns against banks – Carbanak, Odinaff

Nation-States Engaging in Financial Cybercrime– North Korea

North Korean hackers have been linked to multi-million dollar cyber thefts from financial institutions on at least three continents.

- 98 countries with smaller GDP than North Korea
- With sophisticated capabilities and hacking-as-a-service available for purchase, will more countries launch cyber attacks?

Nation-state Threat #2 – Iran

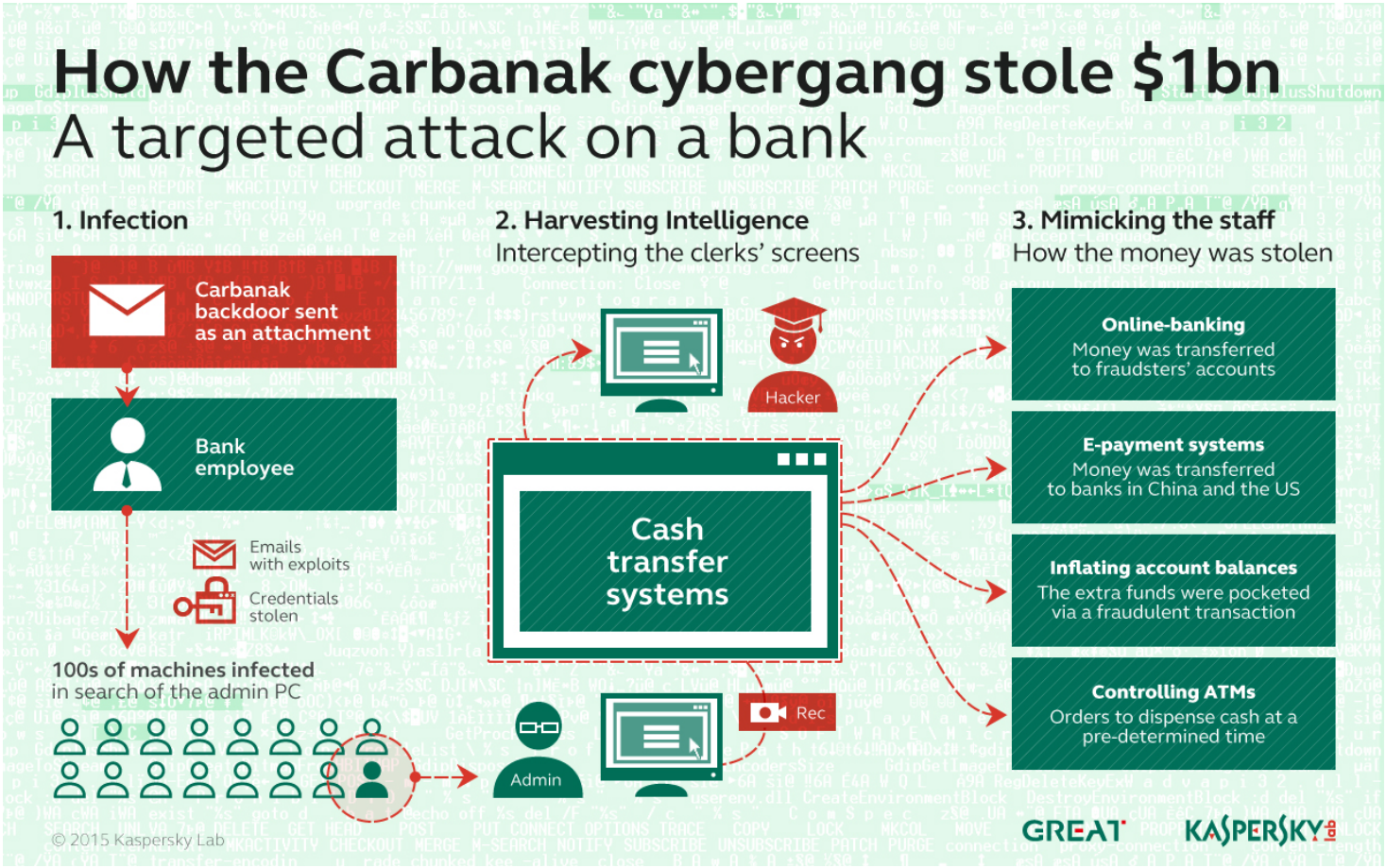
- Operation Ababil – Iran launched the most disruptive cyber campaign in financial sector history 2012-2014

- What will happen if JCPOA fails or the US Government changes its policy toward Iran?

Criminal Groups are Increasingly Sophisticated, Organized

- Nation-state level capabilities are becoming the norm in the top-tier criminal market
  - Russia and Eastern Europe remains the epicenter
    - Russian Business Network, Carbanak, Odinaff
  - Chinese government hackers become mercenaries in Macau
- Data on organized crime is spotty, but there are some illustrative numbers:
  - According to some estimates, 80% of successful cybercrimes are committed by organized crime groups
  - But another estimate says only 20% of cybercriminals are actively affiliated with organized crime groups
  - According to Kaspersky, 1000 cyber-specialists have been recruited into Russian cybercriminal gangs in the last three years, but only 20 individuals are at the core of this network

Criminal Groups Use Multiple Parallel Methods to Monetize Access



Law Enforcement Struggling to Keep Up – The UK as an Example

- In the UK, cybercrime prosecutions rose 34% in 2015.
- **To a total of *61…***
- By comparison, according to the London Police's Action Fraud Unit, ***2.5 million*** incidents of online bank and credit account fraud were reported in the UK last year

Law Enforcement Struggling to Keep Up

Four challenges continue to plague cyber law enforcement:

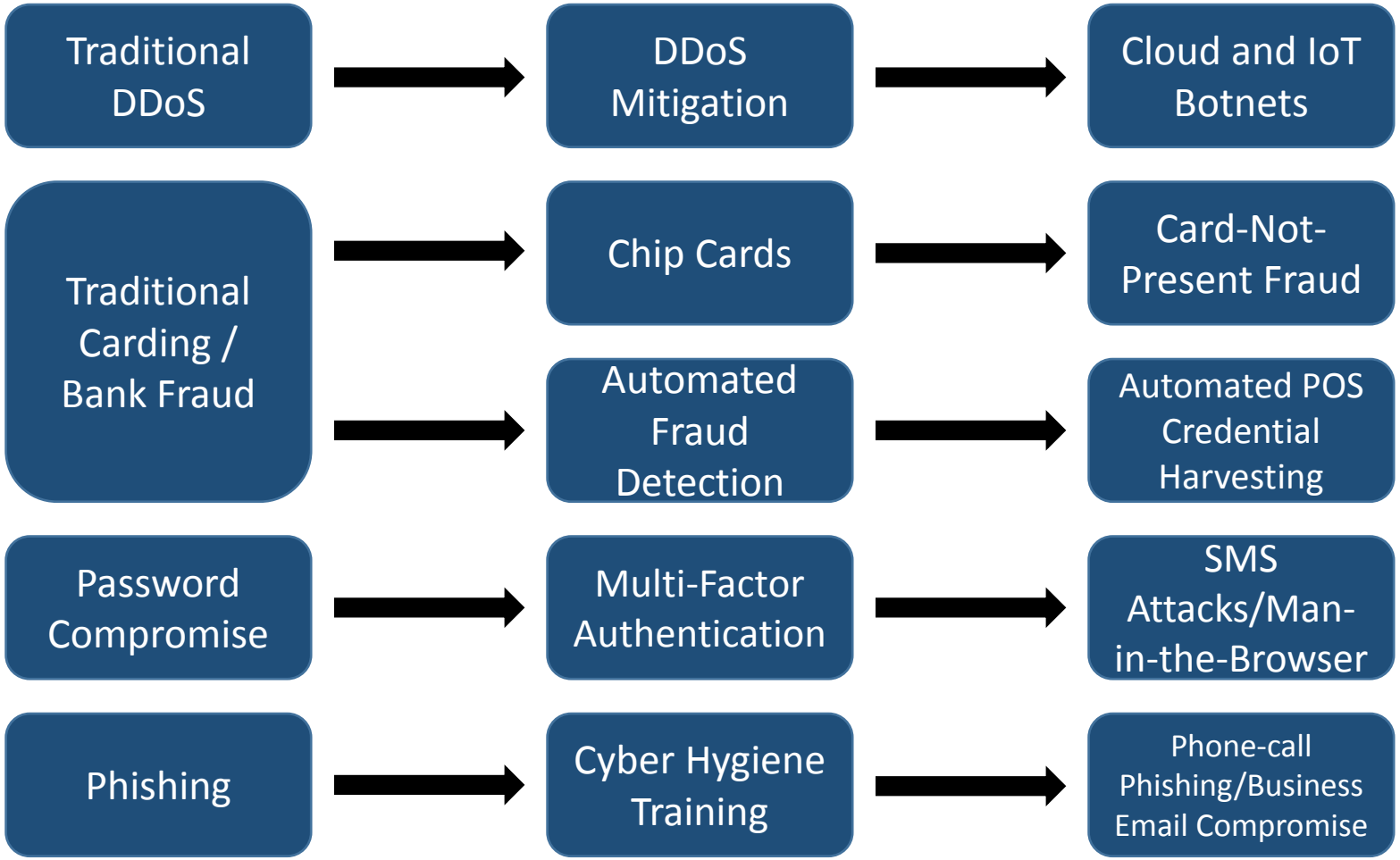
1. Lack of resources
   - Technical specialists, qualified analysts, compute resources, funding, digital evidence training for rank-and-file police
2. Lack of clear authorities to prosecute cybercrime
   - Many countries still have no official cybercrime laws, or have different definitions of cybercrime
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

Cross-Border Issues are Biggest Challenge to Law Enforcement

- 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

3. New Defenses

Attackers Adapt to Defenses, to a Point



Case Study: The Evolution of DDoS Attacks Against Financial Institutions

- The number one threat mentioned by every single bank, cybersecurity company catering to banks, bank regulator, and law enforcement agent interviewed for this study was IoT botnets
- The prevalence of DDoS attacks is staggering. According to one survey, ¾ of financial firms experienced DDoS attacks in 2016, and almost 90% of those victims were subjected to multiple attacks
- One in three banks experiences a major DDoS attack at least once a month

Case Study: The Evolution of DDoS Attacks Against Financial Institutions

Anti-DDoS Measures are Improving

- 9 major DDoS mitigation providers serving the financial sector with over 1Tbps capacity.
- Almost 80% of companies are increasing their investment in DDoS mitigation defenses
- The majority of financial firms employ a hybrid defense including on-site defenses and cloud-based measures

But Attackers are Also Innovating

- Over 500k IoT devices are part of Mirai botnets
- Average DDoS traffic volume topped 200Gbps in late 2016.
- Hybrid DDoS attacks are the new normal
- Fake DDoS extortion is also extremely popular – you don't actually need a botnet to get paid!

Two Interesting Questions from the Research

Is Sophisticated 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 high-level 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 IFIs 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 IFIs 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.

Conclusion

What Does the Threat Landscape Look Like Going Forward?

Attack Methods:

- IoT botnets take DDoS to a new level
- Hybrid attacks will be the norm
- Automated attacks increasingly dominant
- Criminals will rob banks by hacking their customers
- Human vulnerabilities replace software vulnerabilities
- Attackers target seams in the global financial system
- Mobile banking malware is poised for significant growth, especially in the developing world

Adversary groups:

- Nation-state attacks on FIs will continue to grow
- Hacktivism will not present a serious threat for the foreseeable future, but criminals and nation-states may claim hacktivist motives
- Criminals will increasingly target small and medium-sized FIs and FIs in the developing world