MWR InfoSecurity

++

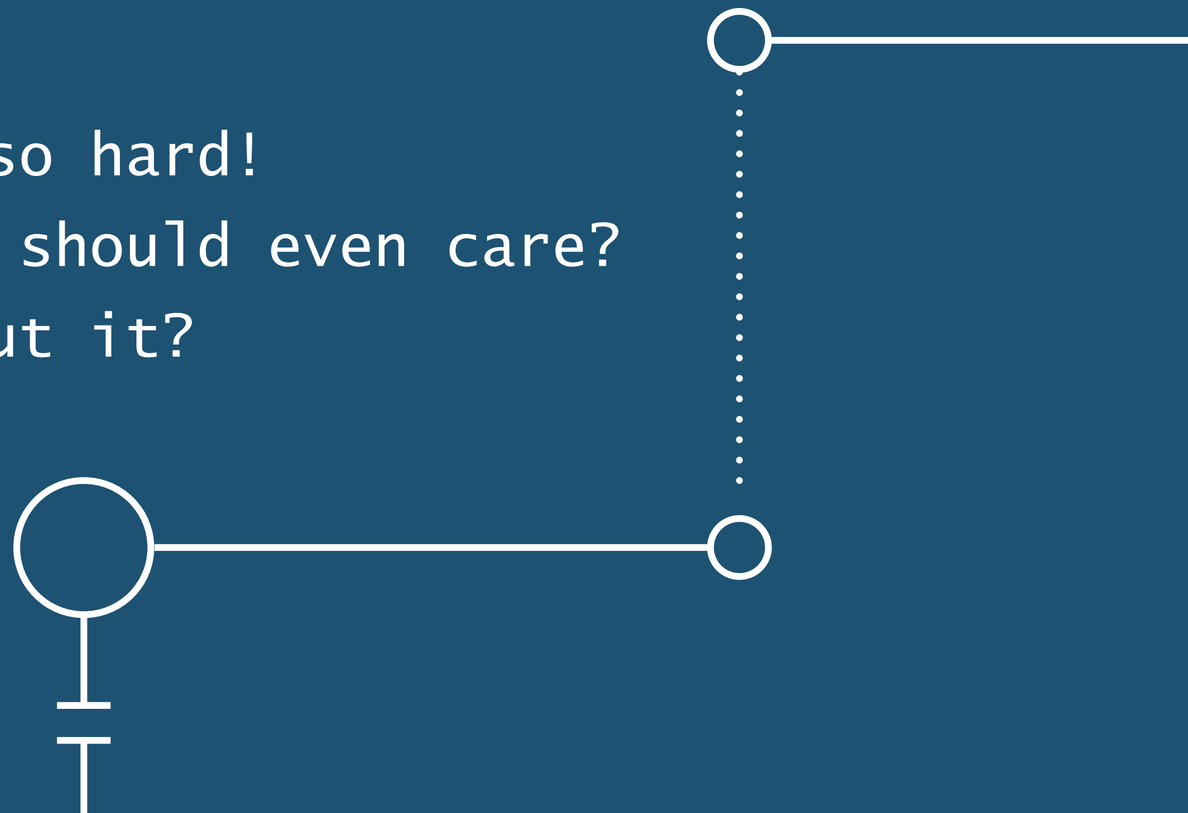
What does it take to steal $81M?

Oliver Simonnet

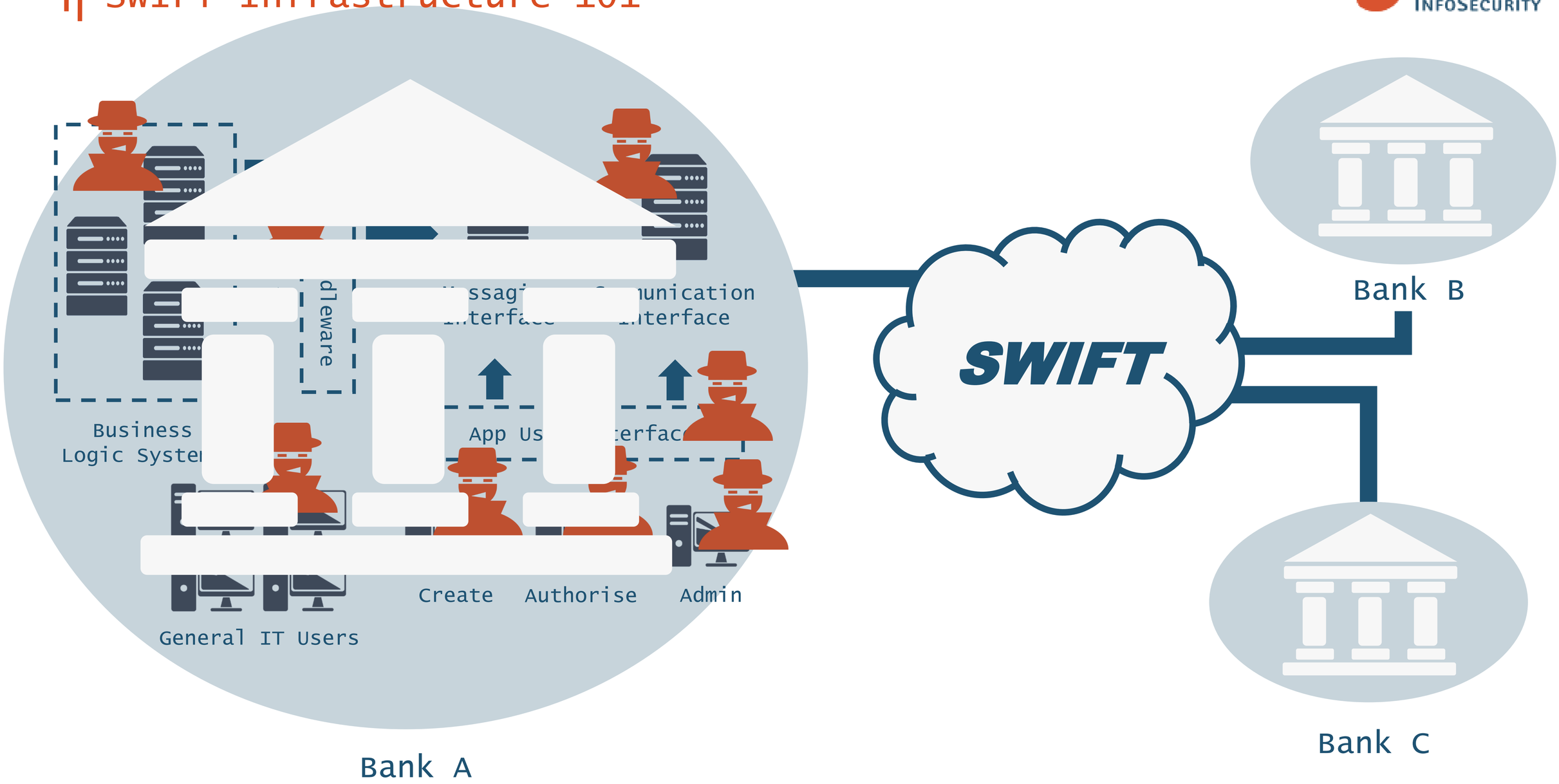
Swiss Cyber Storm – 2018

What are we going to talk about?

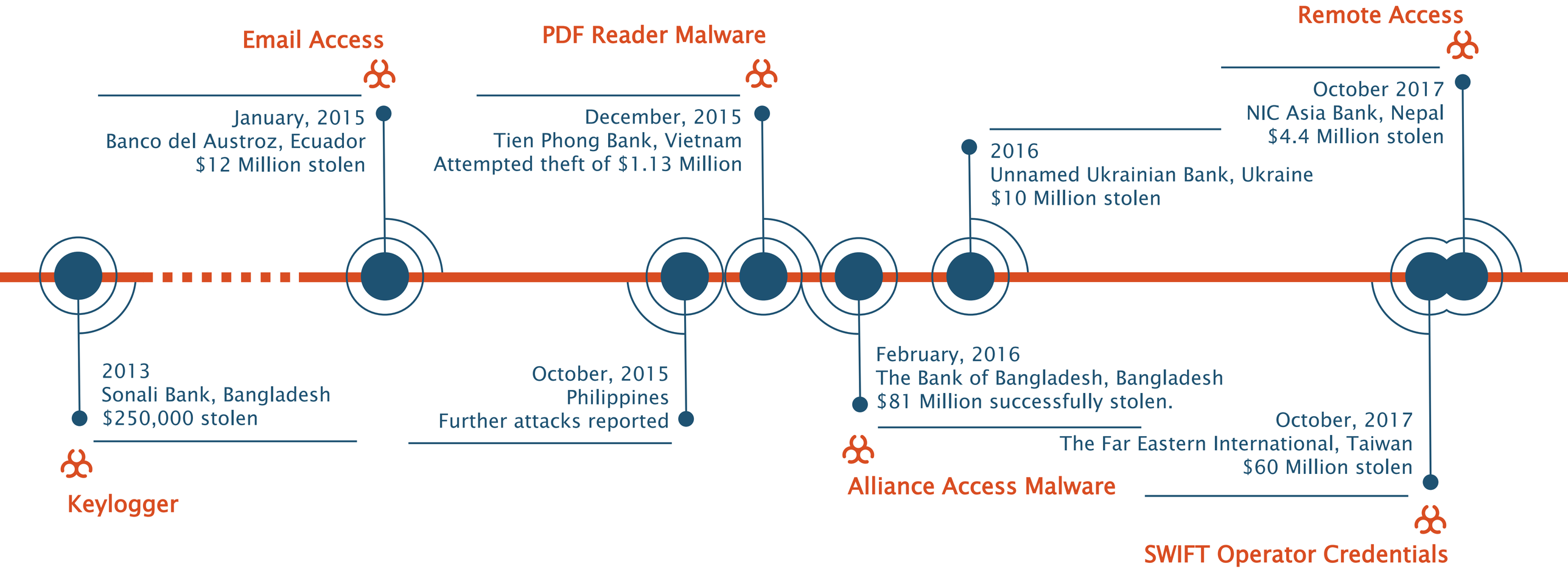
+ SWIFT from an attackers perspective
+ Attacker TTPs
+ Why it’s so easy!
+ Oh, I mean, why it’s so hard!
+ In that case, Why you should even care?
+ What’s being done about it?



SWIFT Infrastructure 101



SWIFT Related Attacks (2013 – 2017)



2018

February 2018 – $6M
Unknown Russian bank, Russia

March 2018 – Prevented!
Malaysia's central bank, Malaysia

August 2018 – $13.5M
Cosmos Bank, India

October 2018 – FireEye Reports:
NK used SWIFT network to try and steal $1.1B
from at least 16 institutions since 2014

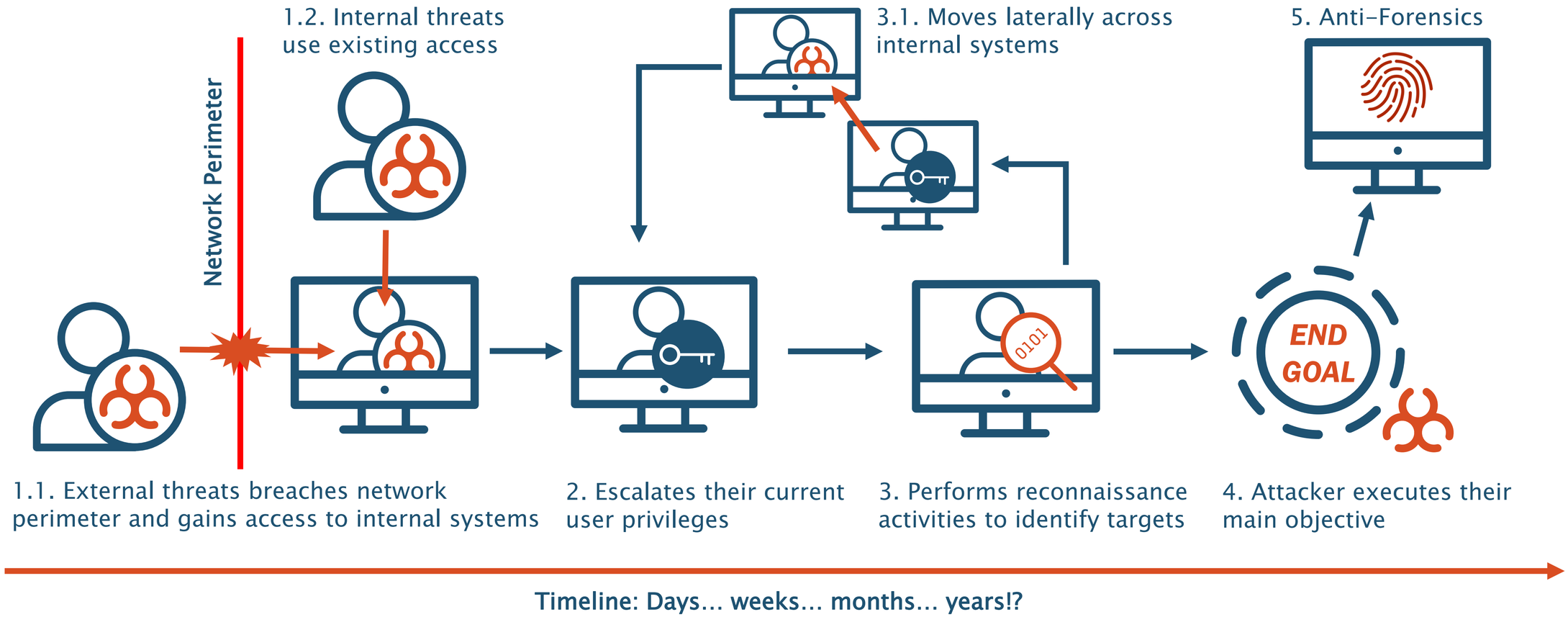
February 2018 – $2M
City Union Bank, India

June 2018 – $10M
Banco de Chile, Chile

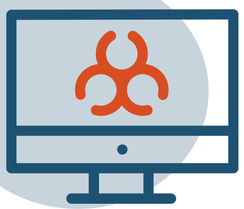
August 2018 – SWIFT Warning
Multiple catalogued attempts to hack
into bank systems to issues
fraudulent SWIFT messages

MWR InfoSecurity

Attacker TTPs



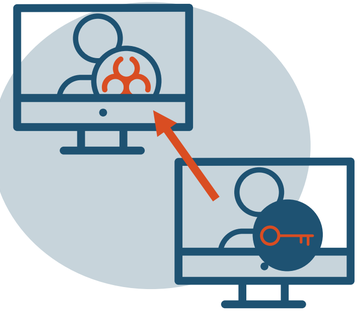
Attacker TTPs



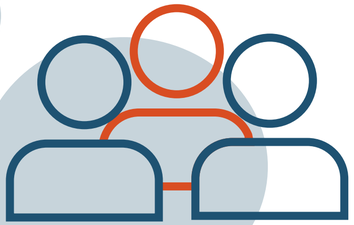
Malware

Credential Compromise

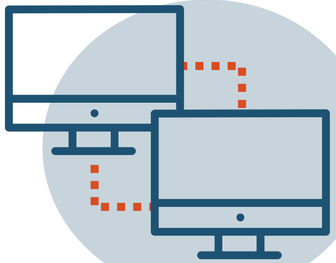
Phishing



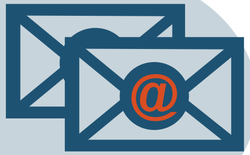
Lateral Movement



Possible Insider Threat



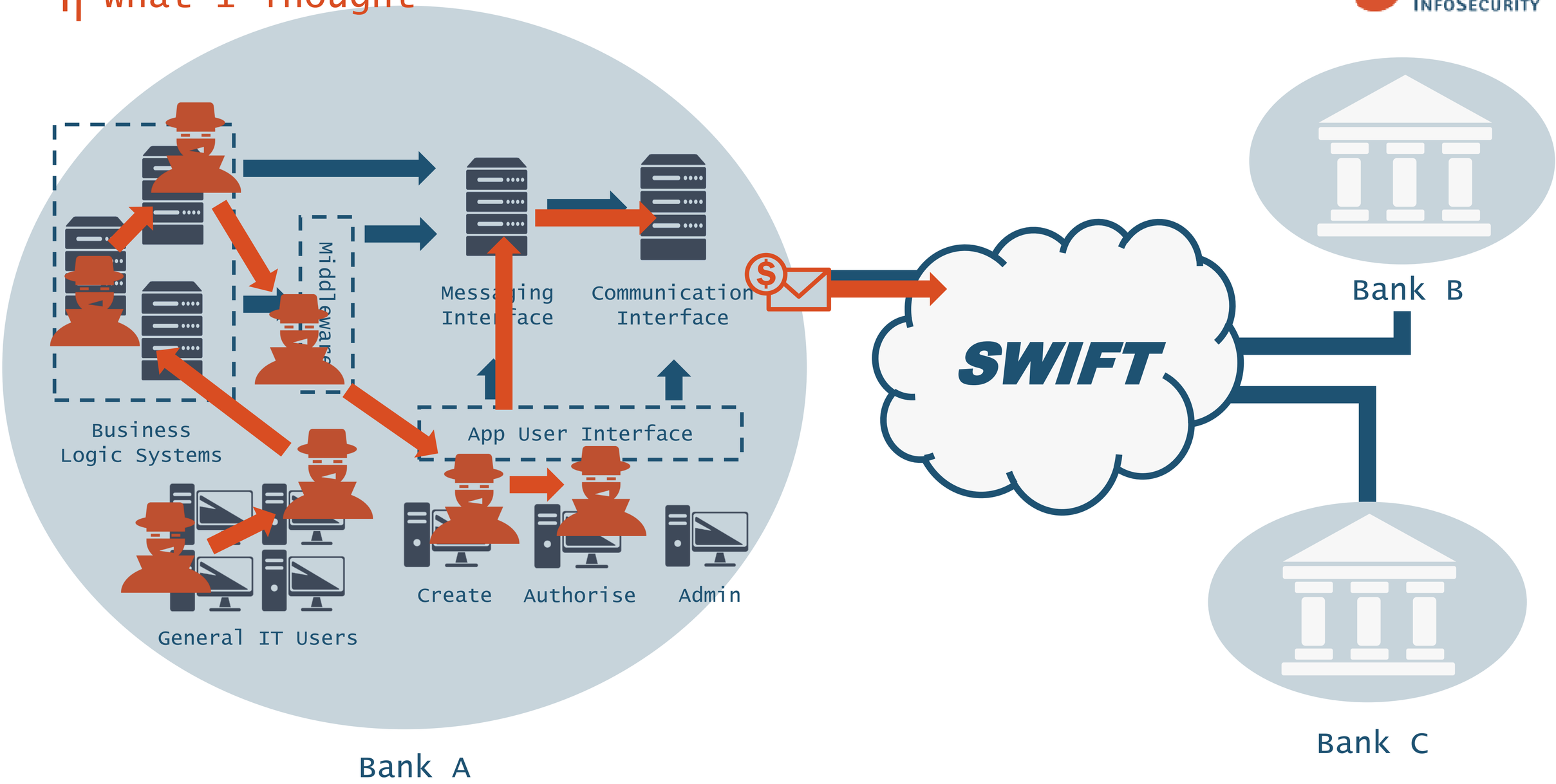
Remote Access



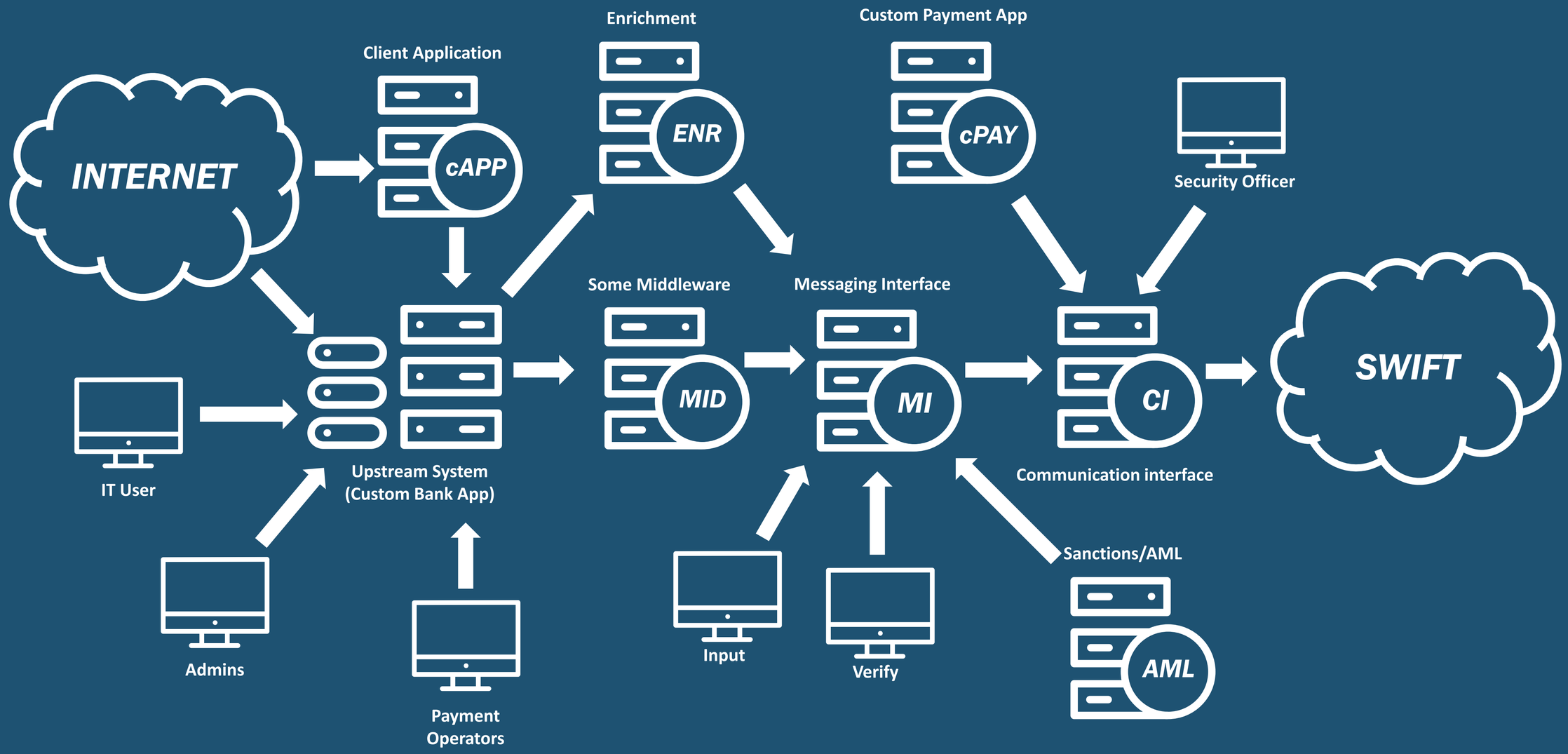
Email Access

Unknown

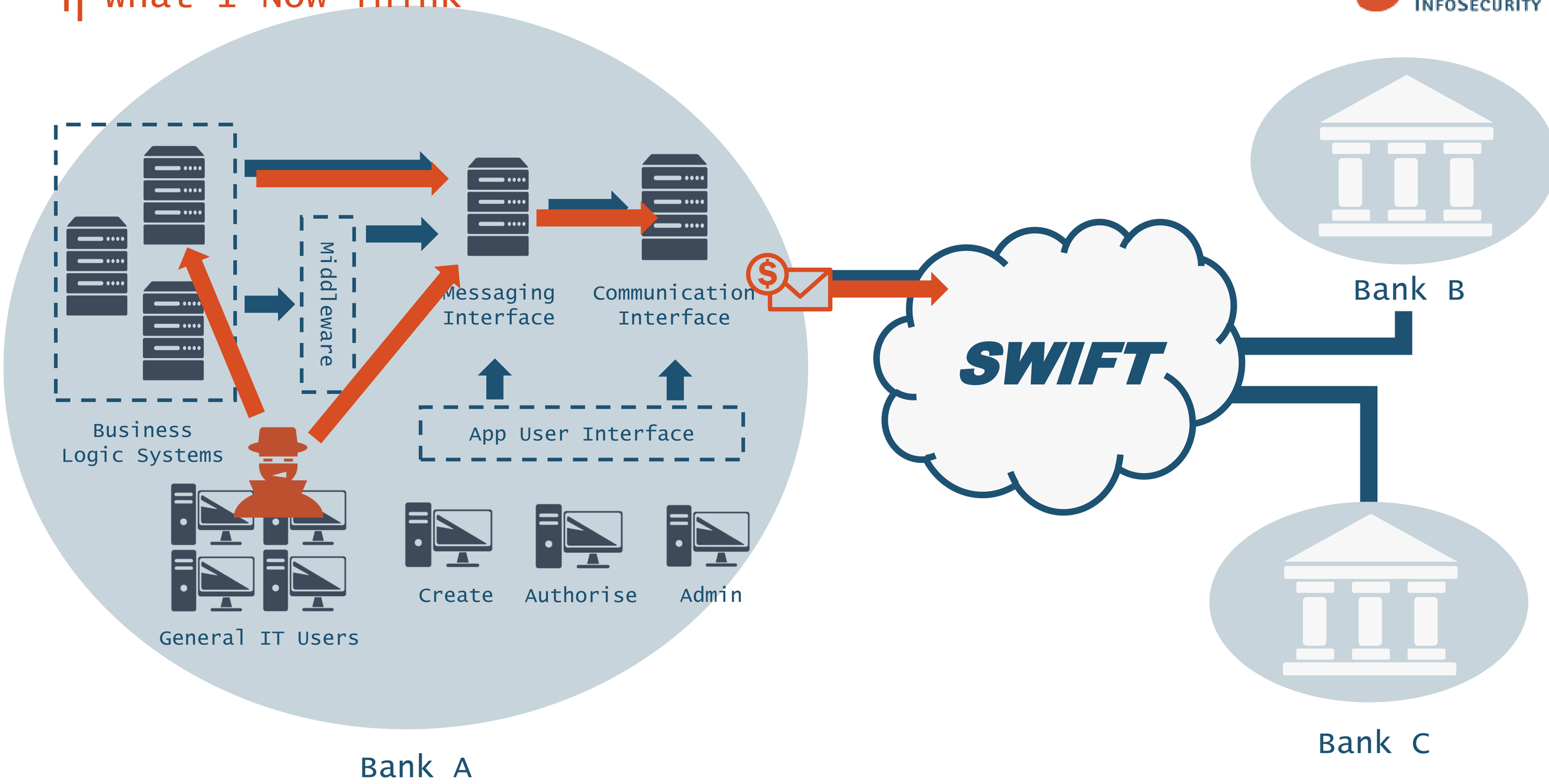
What I Thought



What I Discovered

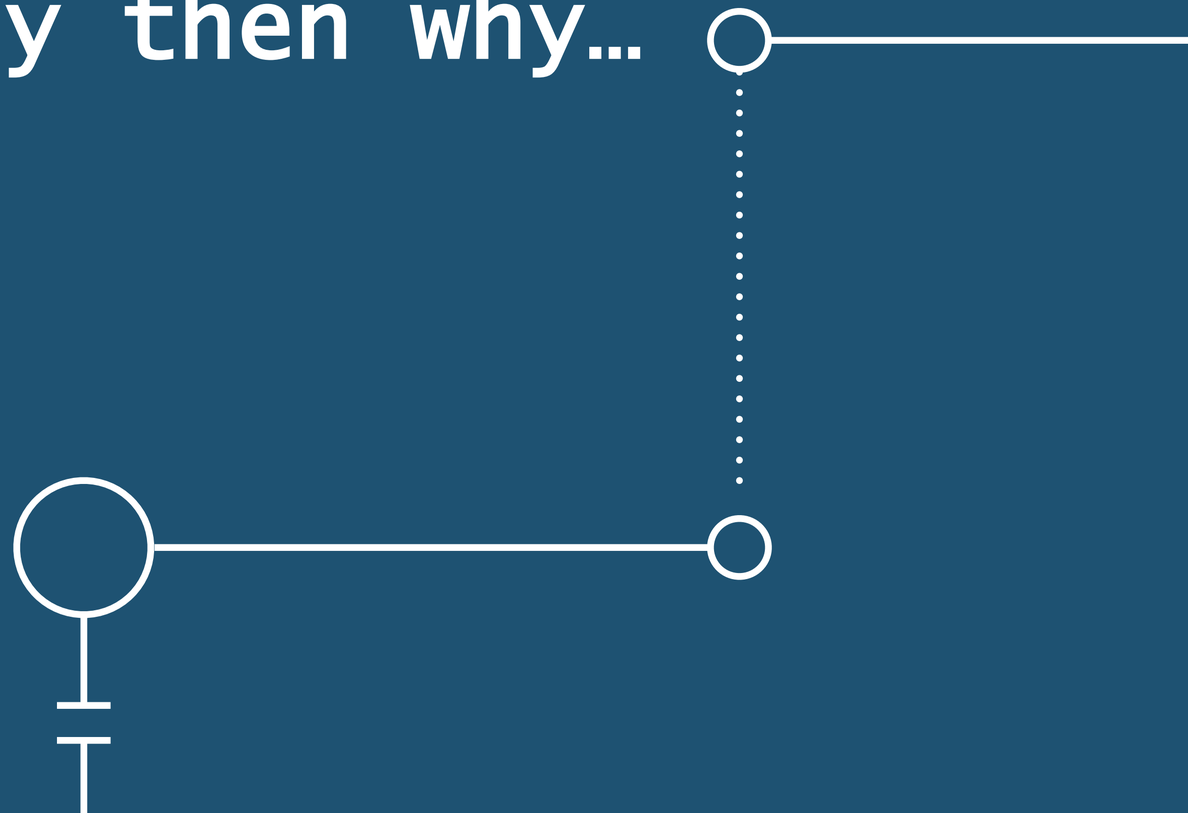


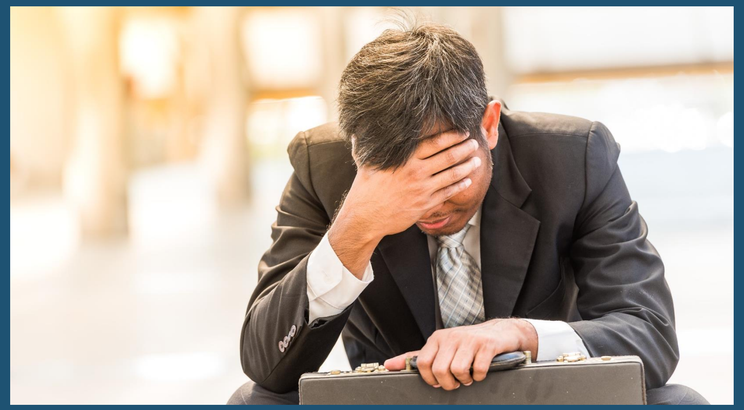
What I Now Think



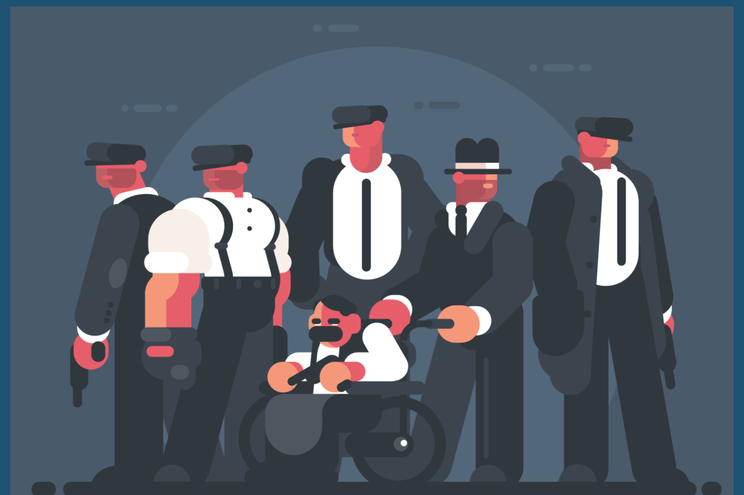
MWR INFOSECURITY

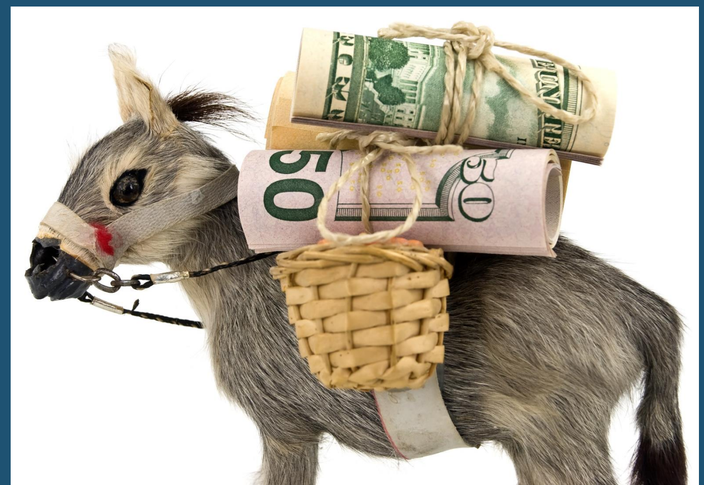
OK, if it's so easy then why…





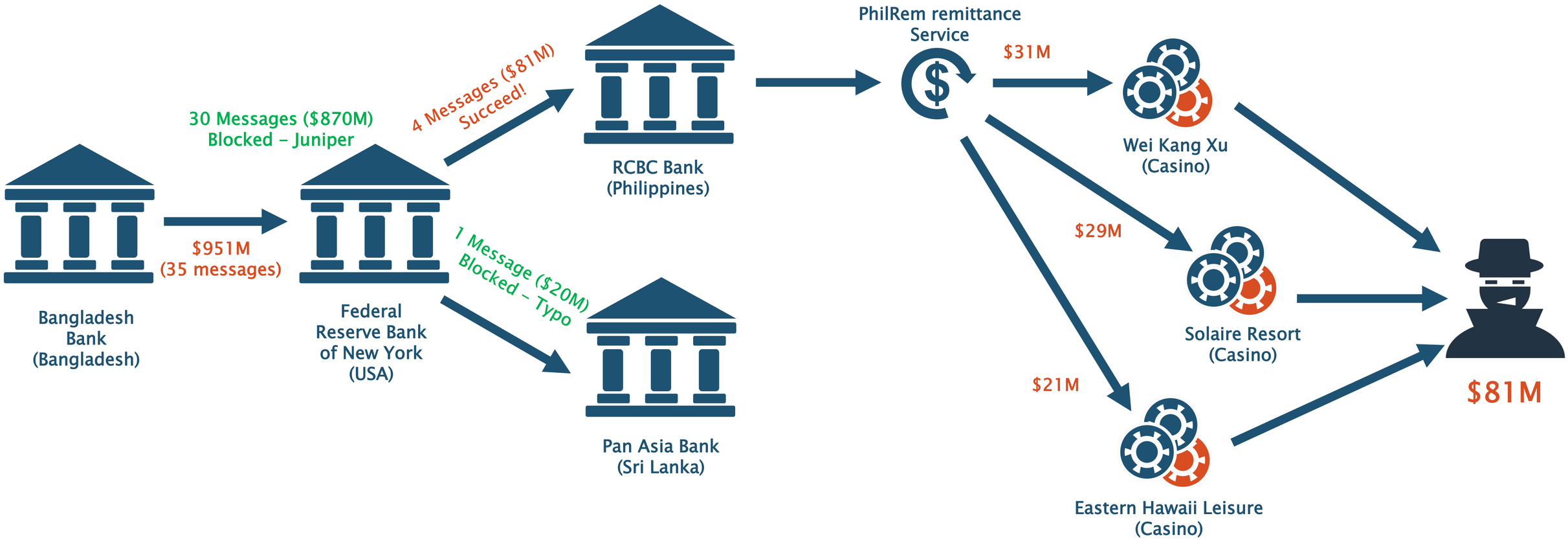
Well…





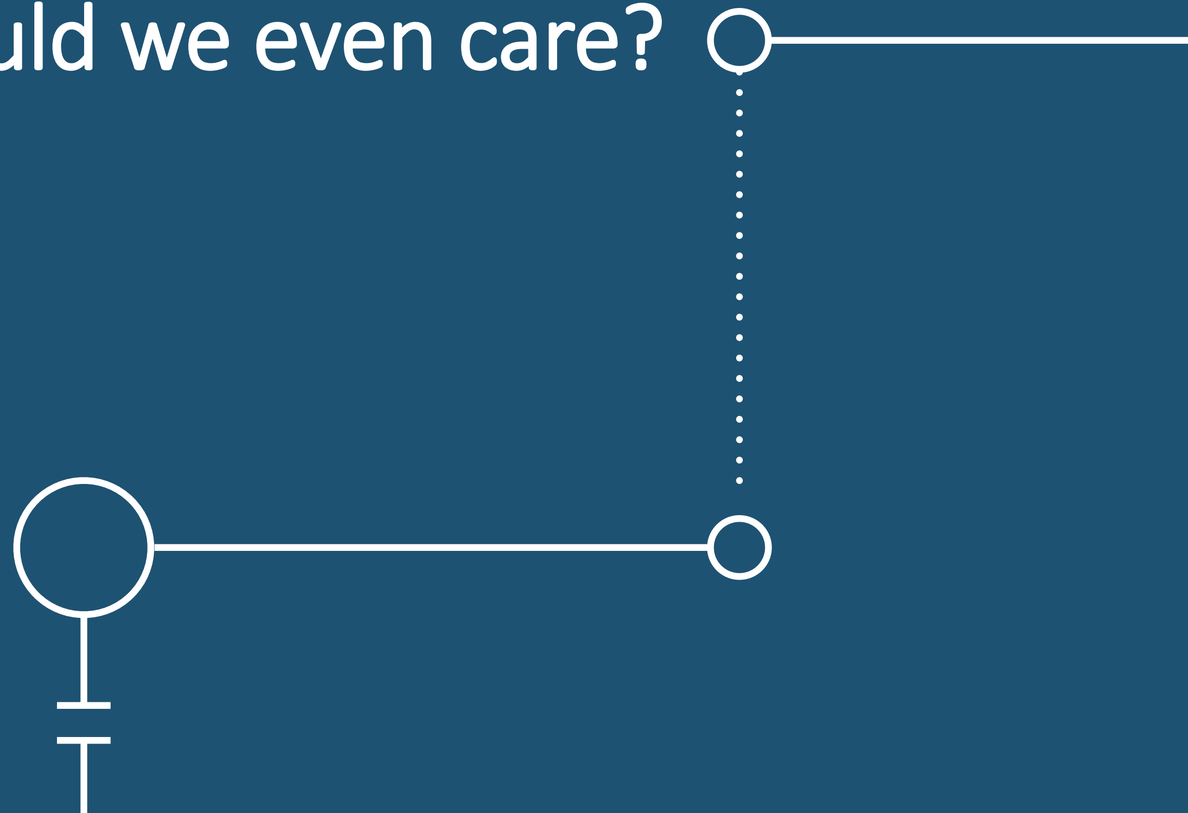
BCB Heist – Funds Journey

++



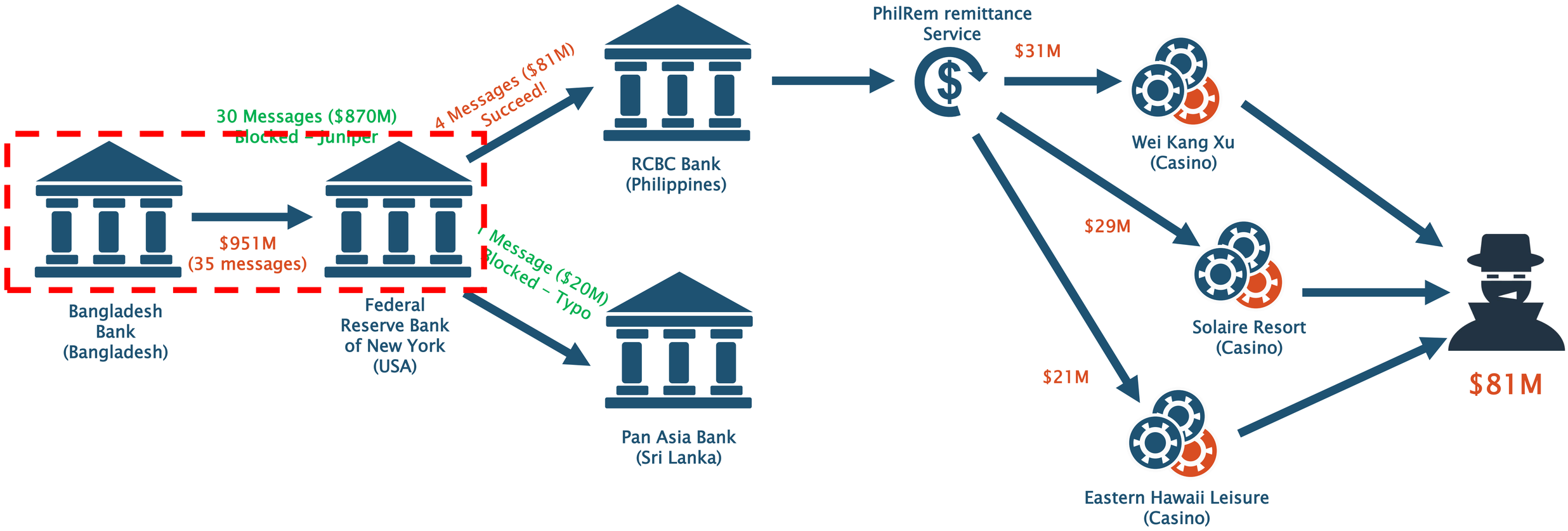
MWR INFOSECURITY

Well in that case, why should we even care?



BCB Heist – Funds Journey

++



Industry Response

31st March 2017

+ SWIFT Customer Security Programme (CSP)

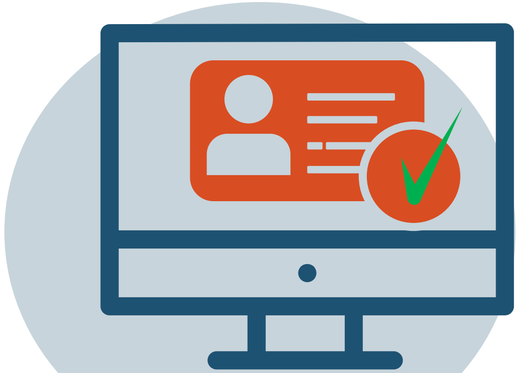
+ Set of 27 mandatory/advisory controls

+ Self-attestation via online portal by 1st January 2018

+ Compliant by 1st January 2019

SWIFT CSP

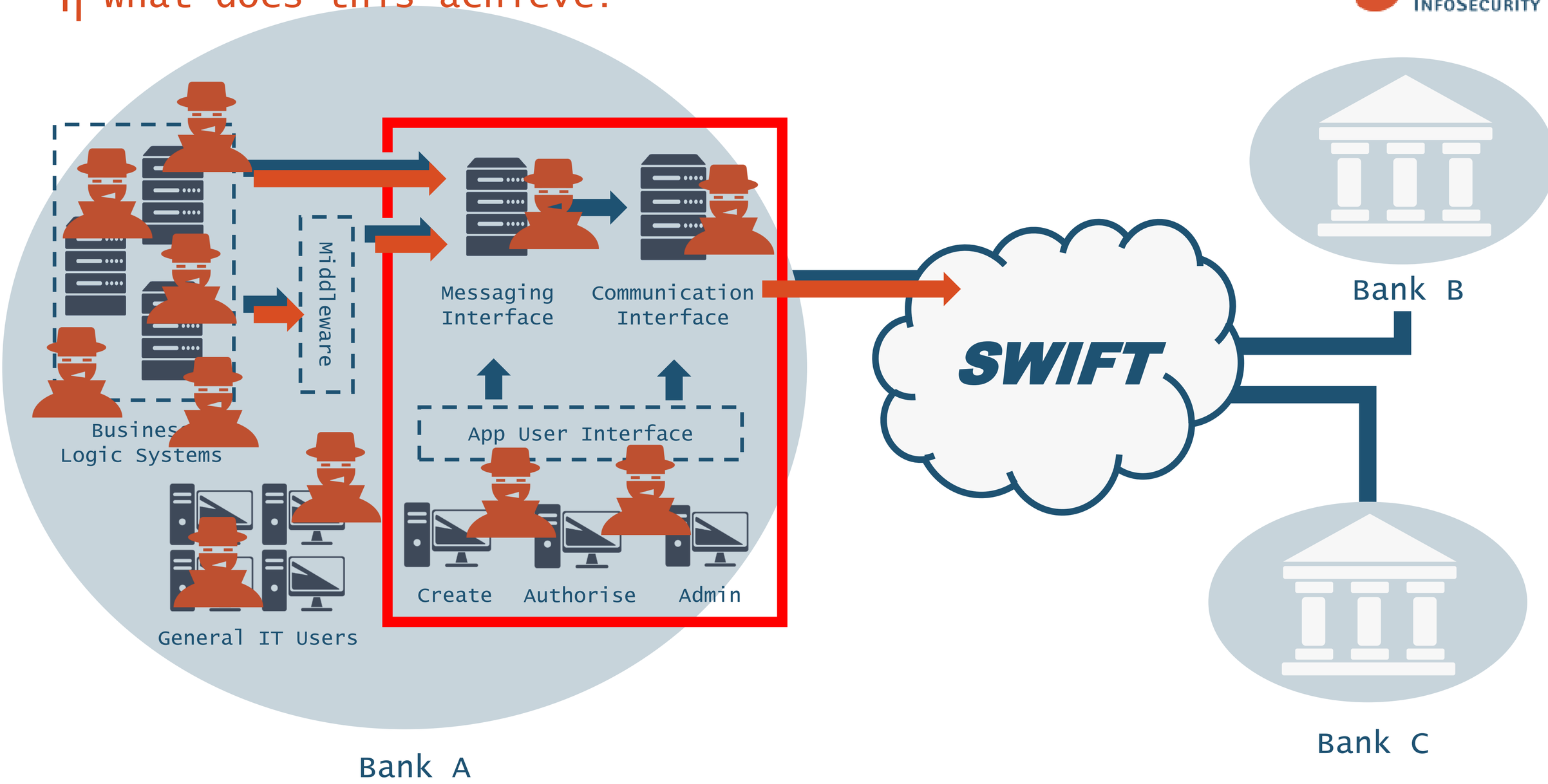
Secure Your Environment



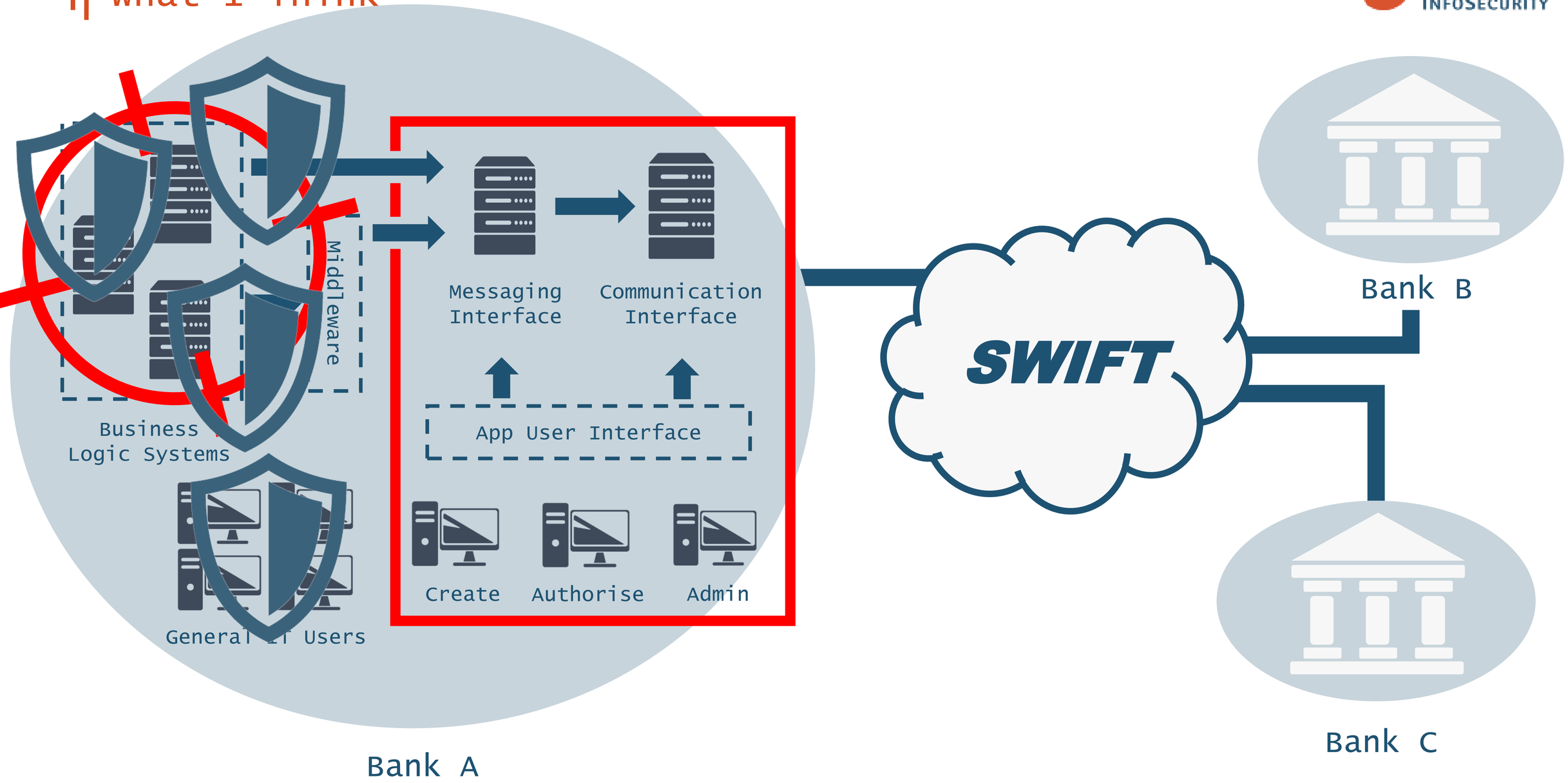
Know and Limit Access

Detect and Respond

What does this achieve?



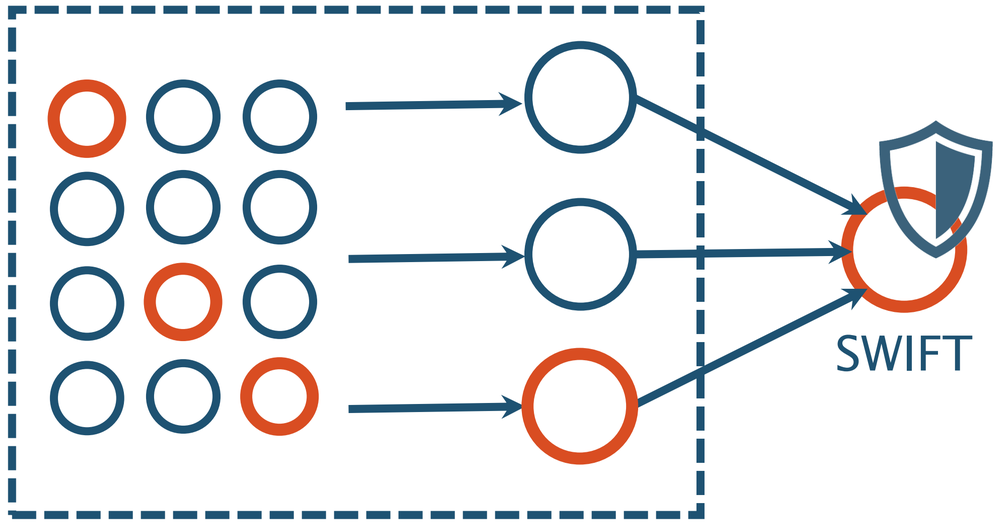
What I Think


Middleware
Business Logic Systems
General IT Users
Messaging Interface
Communication Interface
App User Interface
Create
Authorise
Admin
SWIFT
Bank B
Bank C
Bank A

In Conclusion

++

As we further segregate, isolate and protect SWIFT systems and users, attackers will evolve.

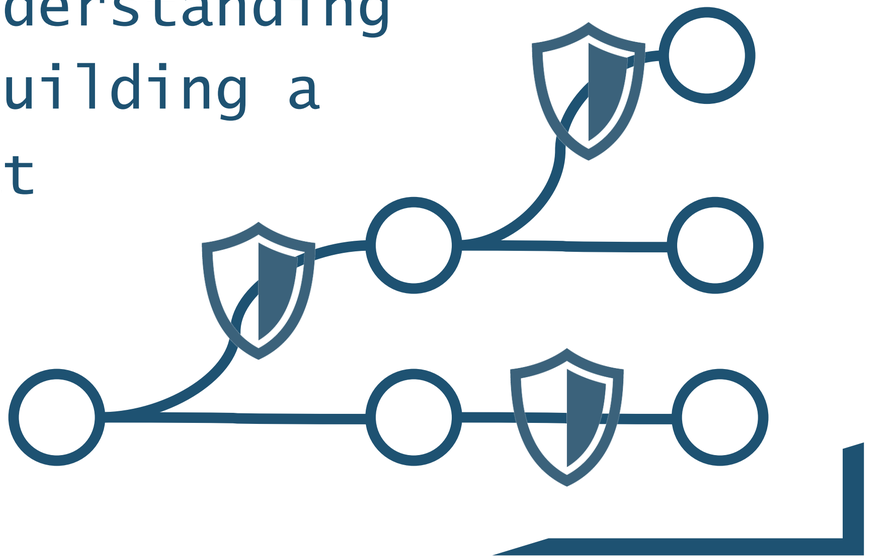


Are upstream systems secure?

In Conclusion

++

Defending payment infrastructure like SWIFT means understanding the attackers and building a defences around that understanding



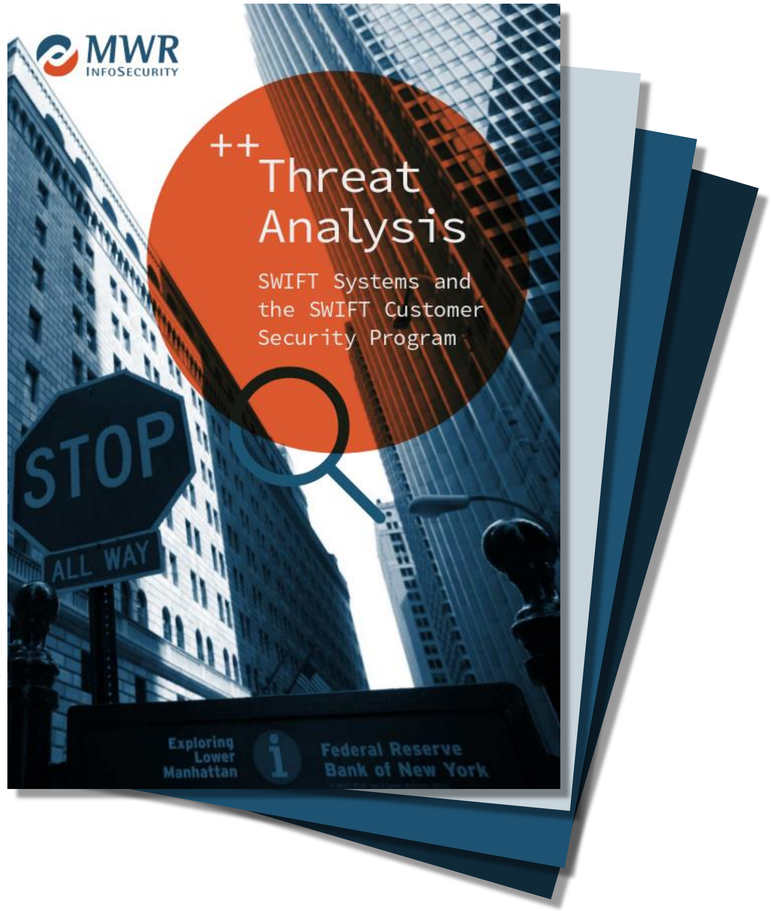
Thank you

++

MWR SWIFT Resources

+ Threat Analysis: SWIFT Systems and the CSP
  https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf

+ Defending SWIFT payment systems from attack
  https://www.mwrinfosecurity.com/our-thinking/defending-swift-payment-systems-from-attack/



MWR InfoSecurity

Questions?