Evolving Cyber Threat Landscape & keeping banks secure in

2022 & beyond

Abeer Khedr
Head of Cyber Security
June 2022

Evolving Threat Landscape : external – internal – third parties

Three Dimensions

Cyber Threats (External)

- Zero-day Threats
- Ransomware, Malware, Spyware
- Threats Targeting Misconfigurations & Unpatched & Vulnerable Assets

Insider Threats

- Fraud
- IT Sabotage
- IP & strategic information theft – accidental or intentional

Third Party Risks "The Extended Enterprise"

- Third party security breaches
- API Risks: Info leakage, lack of integrity
- Regulatory Compliance Impact

Threats prevailing in 2022

- Credential theft from phishing
- **ATO** (Account Takeover Attacks)
- **Bots** (malicious software that runs automated or spreading malware)
- Customer data leakage (, **insecure APIs**, outdate authorization tokens, weak security at third parties)
- **Malware** (access networks to steal data, mobile malware for targeting banking mobile applications)
- overshared **IaaS** and **SaaS** storage (unencrypted/unsecured data stored in cloud environments)
- **Ransomware** (steal data & blackmail organizations)
- Payment **fraud** (from **Vishing** & other **techniques**)

Security risks Introduced by New Technology

- **Open banking** security risks ranging from API attacks that steal customer data.
- **Facial recognition** algorithms that would one method of customer authentication come with their security risks as well
- **Disruptive technologies** like blockchain introduce risks relevant to the design of how the blockchain network works most prominently

Security Risks Introduced By New Technology

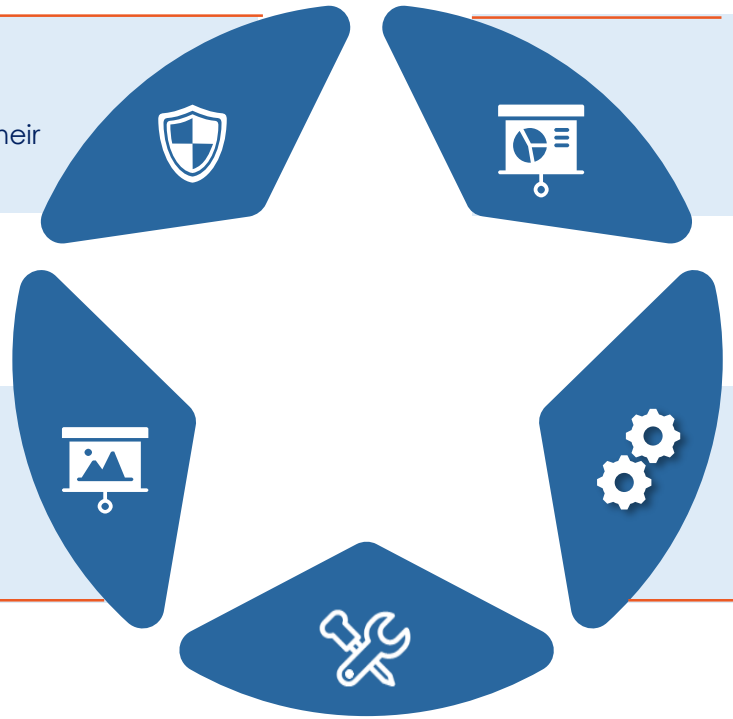
New Technology & applications design introduce new risks that must be addressed

Open Banking Security Risks:

- API attacks
- Attacks on Fintech companies
- Privacy concerns from customers on how their data will be used in this trust relationship

New Architecture Trends - Containerization

- Compromised API server
- Image vulnerabilities
- Inter-container network traffic is encrypted so while this is important yet it makes it difficult to detect malware spreading from an infected container to other containers in the architecture



Facial recognition Algorithms:

- Compromise of systems storing this biometric data is far more dangerous than compromise of a list of passwords
- More critically, accuracy of the algorithm detection is a key risk

Work From Home Arrangements

- Use of conferencing applications Lack of security controls of a virtual meeting
- Employees use of personal devices for work
- Unsecure home connection
- Employees may not observe confidentiality in their home setup

Disruptive Technologies (e.g.: Blockchain):

- Routing attacks where hackers attempt to intercept data transferred in real time over the network
- 51% attack whereby the hacker of a compromised node can impact the integrity of the chain and could result in reversal of transactions

Legal & Regulatory Outlook

Central Bank of Egypt Regulations

1. A new comprehensive cyber security framework has been issued recently by CBE. The framework ihas a set of more than 300 controls that span people-process-technology dimensions
2. CBE regulation is expected to be released regulating third parties & fintech in additional to regulations related to digital banks & customer onboarding
3. Continuing compliance is required with existing CBE regulations (of relevance: internet banking & mobile payment regulations as well as internal control and customer rights protection regulations)

Local legal Frameworks

1. New Banking Law No. 194, 2020 (grace period: 3 years)
2. Anti-Cyber and Information Technology Crimes Law No. 175, 2018
3. E-signature law issued 2004

Applicable International Standards

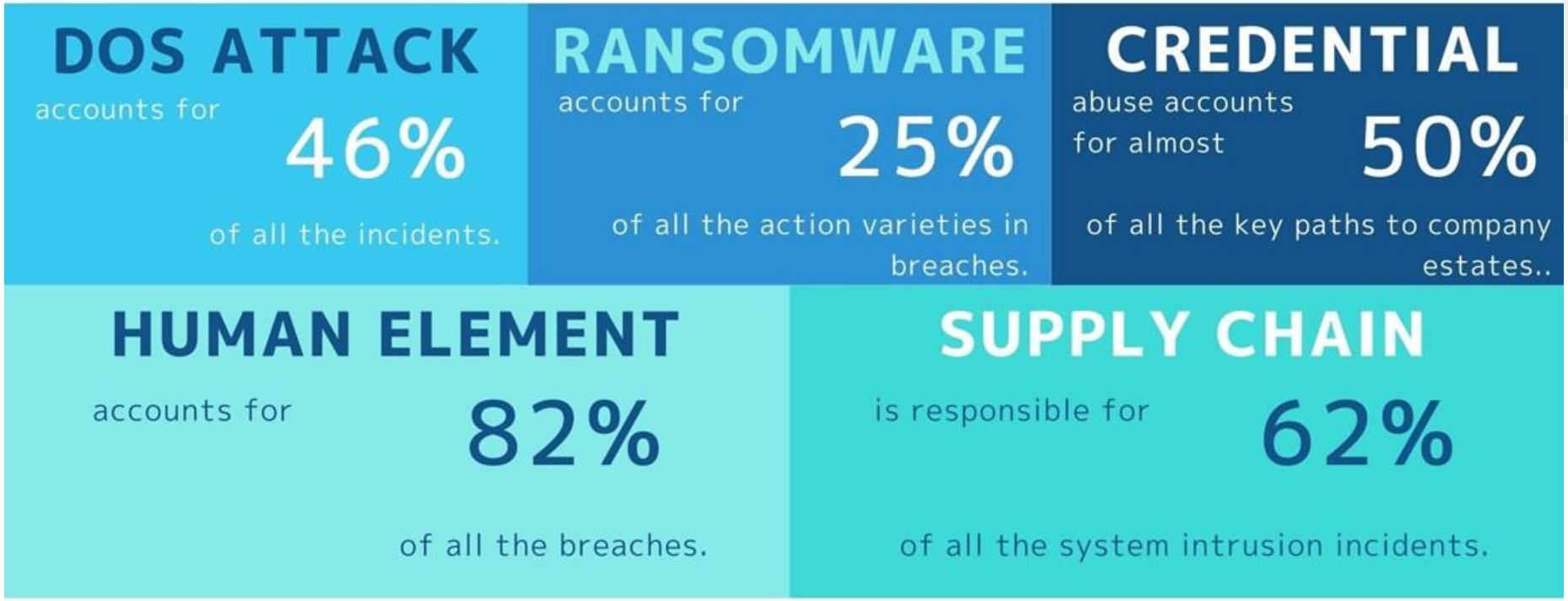
1. SWIFT Customer Security Program (CSP)
2. PCI DSS (Payment Card Industry Data Security Standard)
3. ISO 27001

Examples of Cybersecurity & Privacy Regulations

International Laws & Regulations

- New York, United States: NY Department of financial services cyber security standard –
- UAE: New data protection law issued this year; regulator audit to verify compliance.
- Saudi Arabia: SAMA cyber security regulation.
- United Kingdom: UK-GDPR.
- China: Data Security Law - PIPL or Personal Information Protection Law

Actual breaches tell us where to focus the attention



Source: 2022 Data Breach Investigation Report (DBIR) | Verizon

Keeping banks secure amidst this threat landscape

Addressing the human element

- Invest in customer & employee creative security awareness campaigns
- Brand protection services are essential to complement awareness efforts
- Analyze onboarding & other process flows with a fraudster mindset
- Careful study of user access rights & IAM/PAM implementations
- Make use of UBA (user behavior analytics) to profile user behavior & detect patterns of violations; similarly EFM solutions for customers

Application security & the supply chain risk

- Embed secure design in all stages of SDLC (encryption; anonymization); trace & monitor the software supply chain.
- Change & release management are key.
- Mobile application shielding; also assess identity verification & liveness detection algorithm accuracy
- Source code review is essential
- With open banking, pay special attention to API security & monitoring
- Get assurance over third party security controls (SOC type 2 report or better still security audits)

Infrastructure security & monitoring

- Patching & hardening is key across all infrastructure layers
- Don't forget DDoS shielding
- Anti malware/ransomware protection & detection to be deployed across multiple layers
- Make use of machine learning in detection of network traffic anomalies as well as automating incident response from threat intelligence
- Practice & test incident response & perform table top exercise at executives level

“Security is not a product but a process”

Bruce Schneier

Thank you!