Cyberthreat landscape for fintech and digital financial services

Regional Cybersecurity Summit for Africa
Security learning lab on “Digital financial services”

21 November 2022

Junhyung Park

Co-Editor of X.1150(Security Assurance Framework for Digital Financial Services)

Soonchunhyang University, Korea (Republic of)

SCH SOON CHUN HYANG UNIVERSITY

Contents

01 Introduction

02 Cyberthreat landscape for fintech and digital financial services

03 Security assurance framework for digital financial services

04 Conclusion

Introduction

Introduction

- The rise of fintech and digital financial services has transformed the way we manage and transact money.

- These innovative technologies have made financial transactions more convenient and accessible, but they have also introduced new and complex challenges in the of cybersecurity area.

- Fintech companies and digital financial services providers handle vast amounts of sensitive and confidential information.

- So, the consequences of a cyber attack on a fintech company can be severe, leading to financial losses, reputation damage, and regulatory audit.

- This presentation analyzes cyber threat trends for digital financial services and analyzes the overall ecosystem of digital financial services

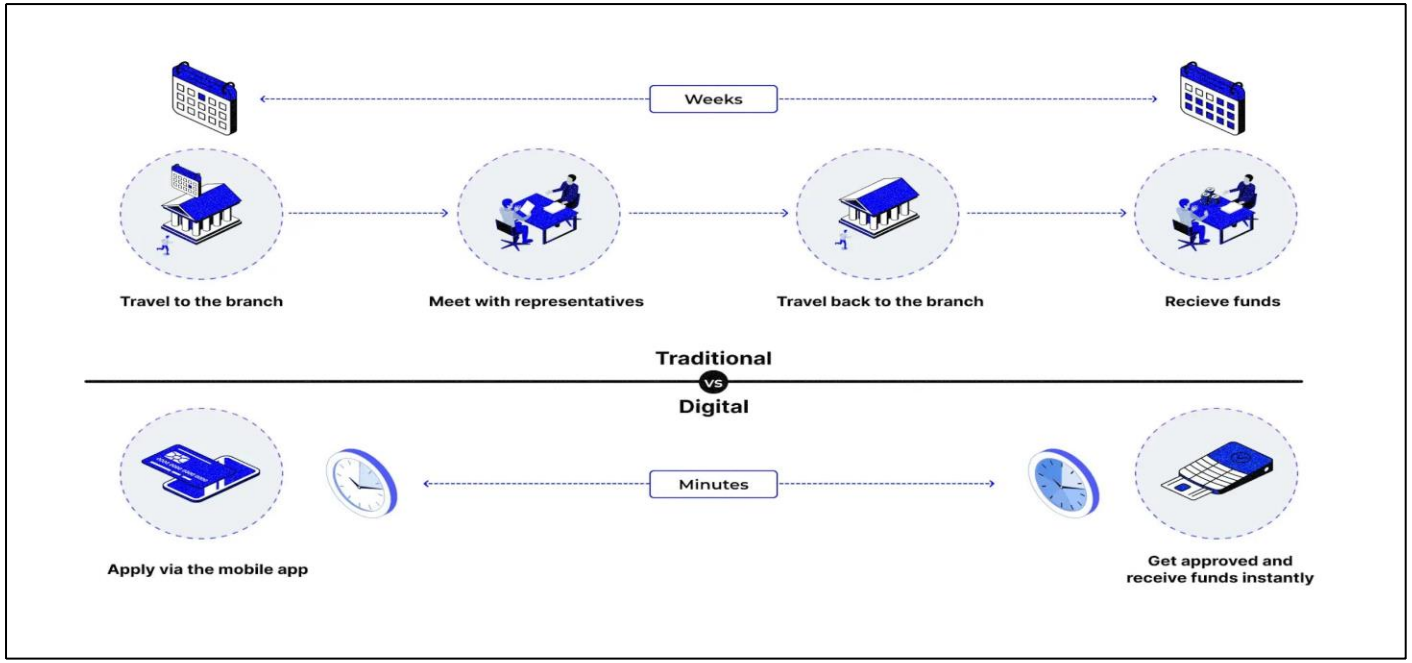
- We also introduce methods to create safe digital financial services by mitigating cyber threats to digital financial services through a security assurance framework.

Digital transformation in financial services

- The financial industry is also experiencing a profound transformation because of digitization.

- These innovative solutions offer a level of efficiency, security, and convenience that is unmatched by traditional banking systems. (e.g. Mobile payment system, Smart contract)

- Financial institutions have seen the potential and high demand for these new technologies and are working hard to implement them.



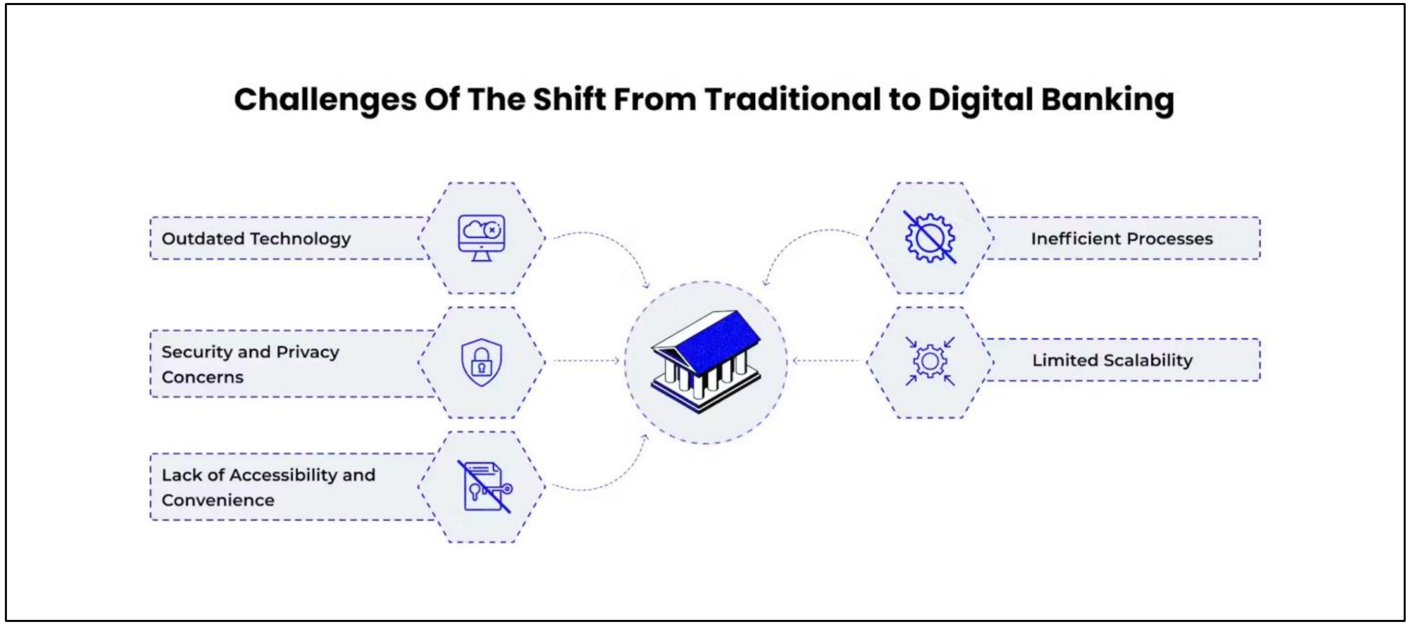
Source: https://maddevs.io/blog/digital-transformation-in-banking-and-financial-services/

Challenges of the shift from traditional to digital banking

- In today's rapidly evolving digital environment, traditional financial institutions must improve their systems to meet customer needs and remain competitive.

- However, there are several challenges facing these system improvements:

  - Outdated Technology
  - Security and Privacy Concerns
  - Lack of Accessibility and Convenience
  - Inefficient Processes
  - Limited Scalability



Challenges Of The Shift From Traditional to Digital Banking

Outdated Technology

Security and Privacy Concerns

Lack of Accessibility and Convenience

Inefficient Processes

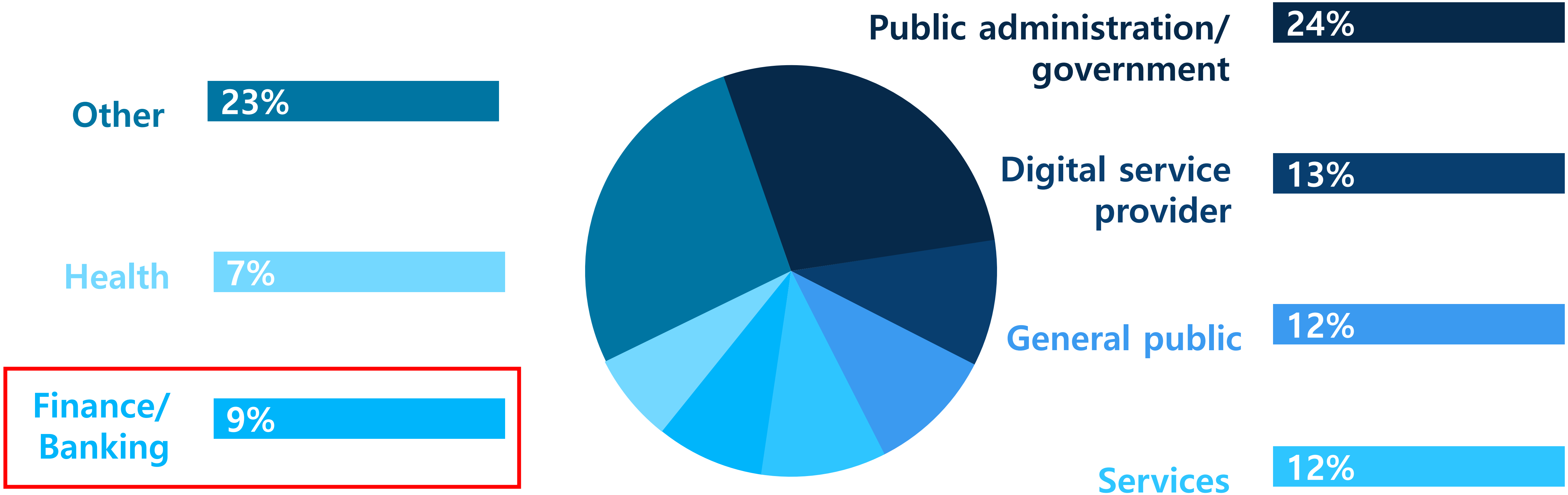
Limited Scalability

Source: https://maddevs.io/blog/digital-transformation-in-banking-and-financial-services/

Cyberthreat landscape for fintech and digital financial services

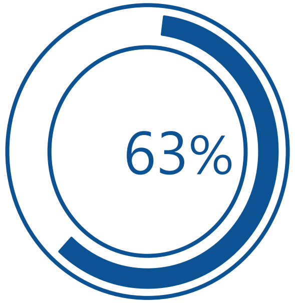
SOON CHUN HYANG UNIVERSITY

Main sectors affected by cybersecurity threat



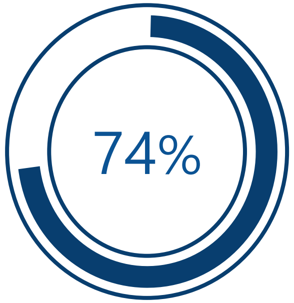
Source: European Union Agency for Cybersecurity 2022

Trends in cyberattacks on the financial sector



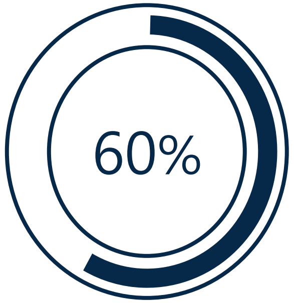
Destructive attacks

63% of financial institutions experienced an increase in destructive attacks, a 17% increase from last year



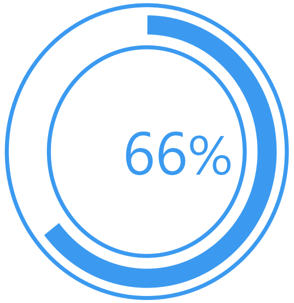
Ransomware attacks

74% experienced one or more ransomware attacks, and 63% of those victims paid the ransom



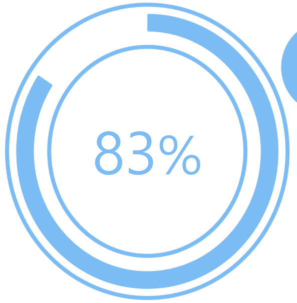
Island hopping

60% of financial institution e xperienced an increase in island hopping



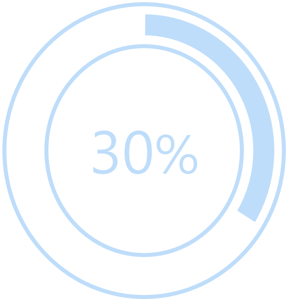
Attacks that targeted market strategies

Two out of three financial institutions experienced attacks that targeted market strategies



Security of cryptocurrency exchanges

83% are concerned with the security of cryptocurrency exchanges



Increase budget

The majority of financial institutions plan to increase their budget by 20-30% this year

Source: European Union Agency for Cybersecurity 2022

Financial services cyber threats

Malware and ransomware attacks

- Ransomware encrypts a victim's files and spread to shared network driver

Ransomware-as-a-Service(RaaS)

- RaaS operates much like legitimate Software-as-a-Services(SaaS)
- The service being provided is ransomware attacks

Social engineering/ Phishing attacks

- These attacks present a formidable threat to financial institutions.
- These attack's cybercriminals manipulate employees into disclosing sensitive information or performing actions that compromise security.

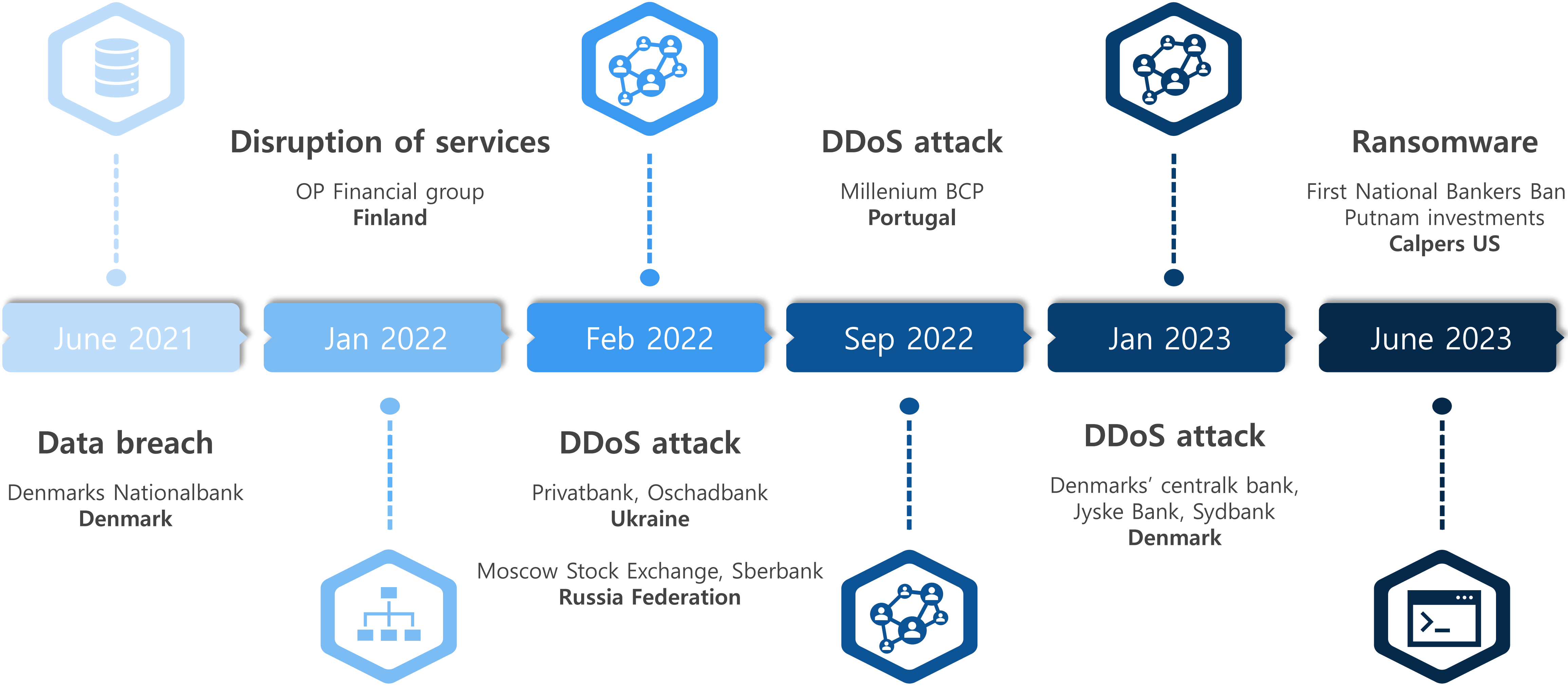
DDos and RDoS attacks

- The primary goal of a DDoS attack is to overwhelm a target system, network, or website with a flood of traffic, rendering it inaccessible to users
- The primary goal of an RDoS attack is to extort money from the victim. Attackers demand a ransom to stop the DDoS attack and restore normal service.

Supply chain attacks

- Supply chain attacks can pose a serious threat to banks and financial institutions, which often have numerous connections with other entities such as insurance companies, vendors, service providers, and other banks

Recent cyber attacks in the financial industry



June 2021

Data breach

Denmarks Nationalbank
Denmark

Jan 2022

Disruption of services

OP Financial group
Finland

Feb 2022

DDoS attack

Privatbank, Oschadbank
Ukraine

Moscow Stock Exchange, Sberbank
Russia Federation

Sep 2022

DDoS attack

Millenium BCP
Portugal

Jan 2023

DDoS attack

Denmarks' centralk bank,
Jyske Bank, Sydbank
Denmark

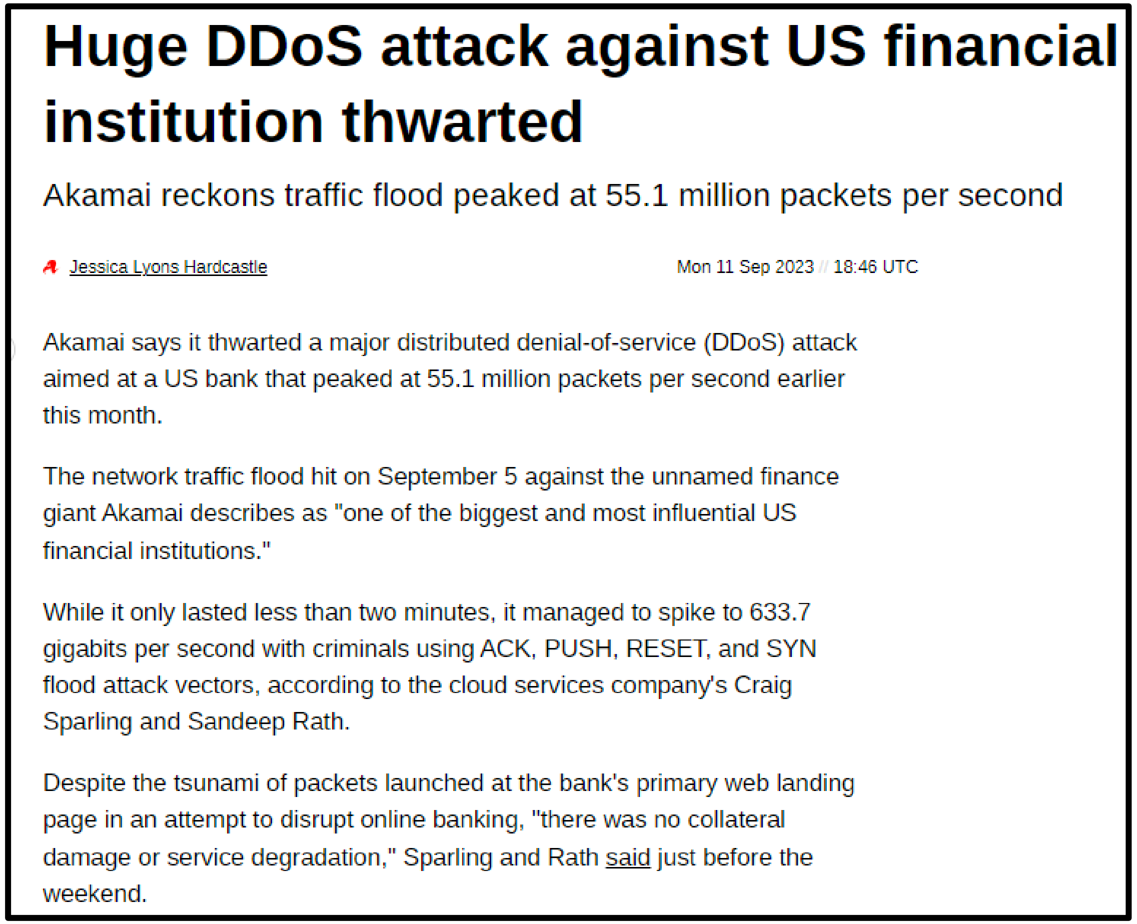
June 2023

Ransomware

First National Bankers Bank,
Putnam investments
Calpers US

Source: Blazeinfosec

Recent cyber attacks in the financial industry



Huge DDoS attack against US financial institution thwarted

Akamai reckons traffic flood peaked at 55.1 million packets per second

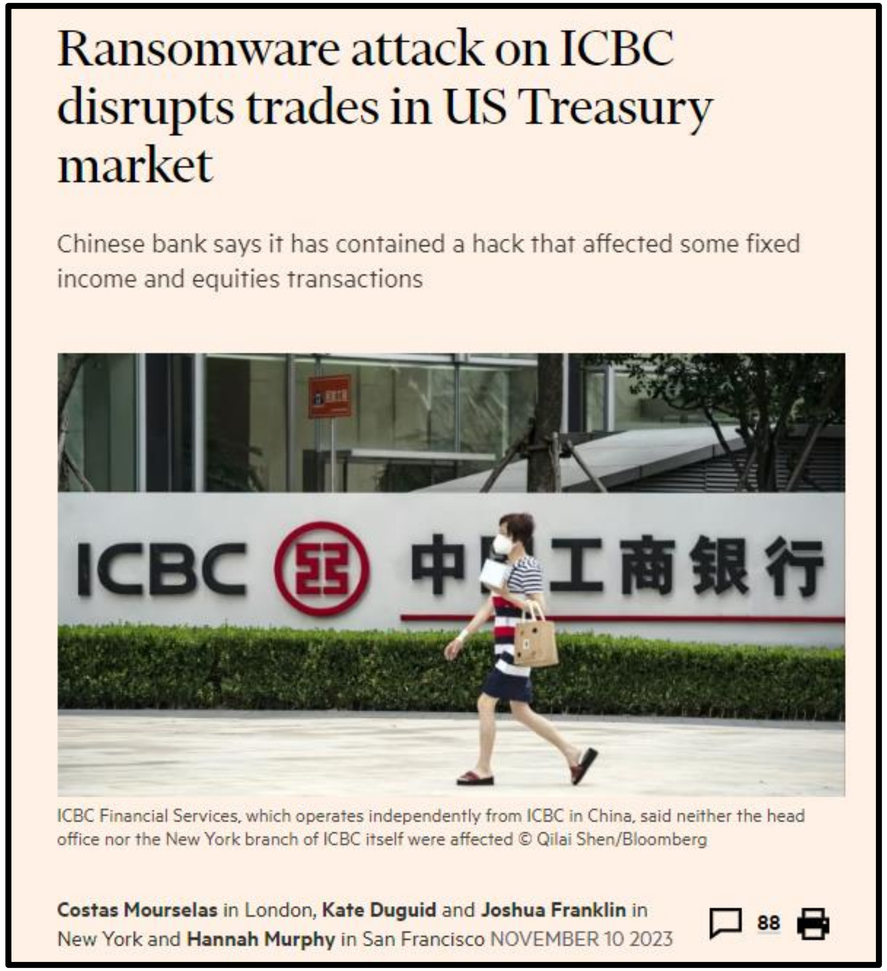
Jessica Lyons Hardcastle Mon 11 Sep 2023 // 18:46 UTC

Akamai says it thwarted a major distributed denial-of-service (DDoS) attack aimed at a US bank that peaked at 55.1 million packets per second earlier this month.

The network traffic flood hit on September 5 against the unnamed finance giant Akamai describes as "one of the biggest and most influential US financial institutions."

While it only lasted less than two minutes, it managed to spike to 633.7 gigabits per second with criminals using ACK, PUSH, RESET, and SYN flood attack vectors, according to the cloud services company's Craig Sparling and Sandeep Rath.

Despite the tsunami of packets launched at the bank's primary web landing page in an attempt to disrupt online banking, "there was no collateral damage or service degradation," Sparling and Rath said just before the weekend.



Ransomware attack on ICBC disrupts trades in US Treasury market

Chinese bank says it has contained a hack that affected some fixed income and equities transactions

ICBC Financial Services, which operates independently from ICBC in China, said neither the head office nor the New York branch of ICBC itself were affected © Qilai Shen/Bloomberg

Costas Mourselas in London, **Kate Duguid** and **Joshua Franklin** in New York and **Hannah Murphy** in San Francisco NOVEMBER 10 2023

88

Security assurance framework for digital financial services

SOON CHUN HYANG UNIVERSITY

Security assurance framework for digital financial services

X.1150 (ex. X.saf-dfs)

Title

- Security assurance framework for digital financial services

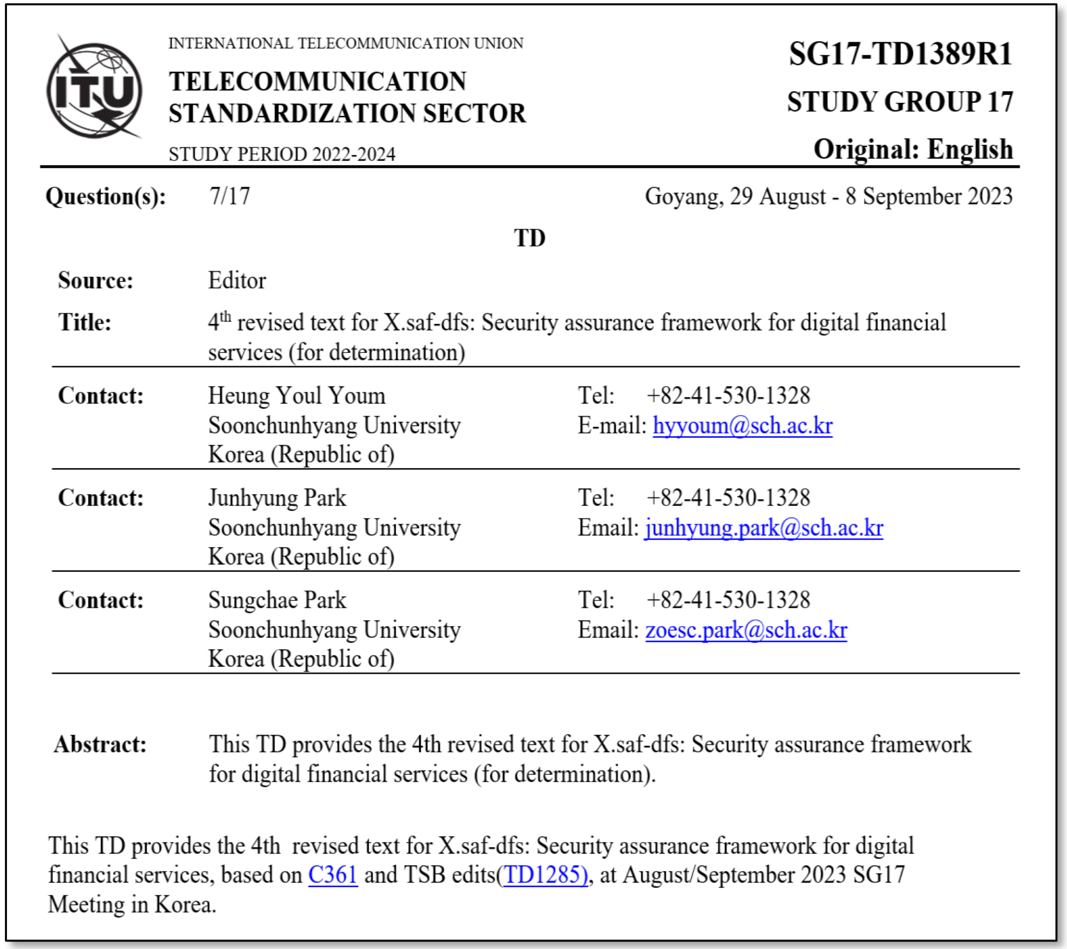
Editors

- Prof. Heung Youl YOUM
- Mr. Junhyung Park
- MS. Sungchae Park

History

- Base line text published from ITU FIGI (Apr 2021)
- New Work Item Proposal (Aug 2021)
- TAP Determined (Sep 2023)
- TAP Consultation (On-going)

Provides an overview of the security threats and vulnerabilities facing the stakeholders in DFS ecosystem.



INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2022-2024

SG17-TD1389R1
STUDY GROUP 17
Original: English

Question(s): 7/17 Goyang, 29 August - 8 September 2023

TD

Source: Editor

Title: 4th revised text for X.saf-dfs: Security assurance framework for digital financial services (for determination)

Contact: Heung Youl Youm
Soonchunhyang University
Korea (Republic of)
Tel: +82-41-530-1328
E-mail: hyyoum@sch.ac.kr

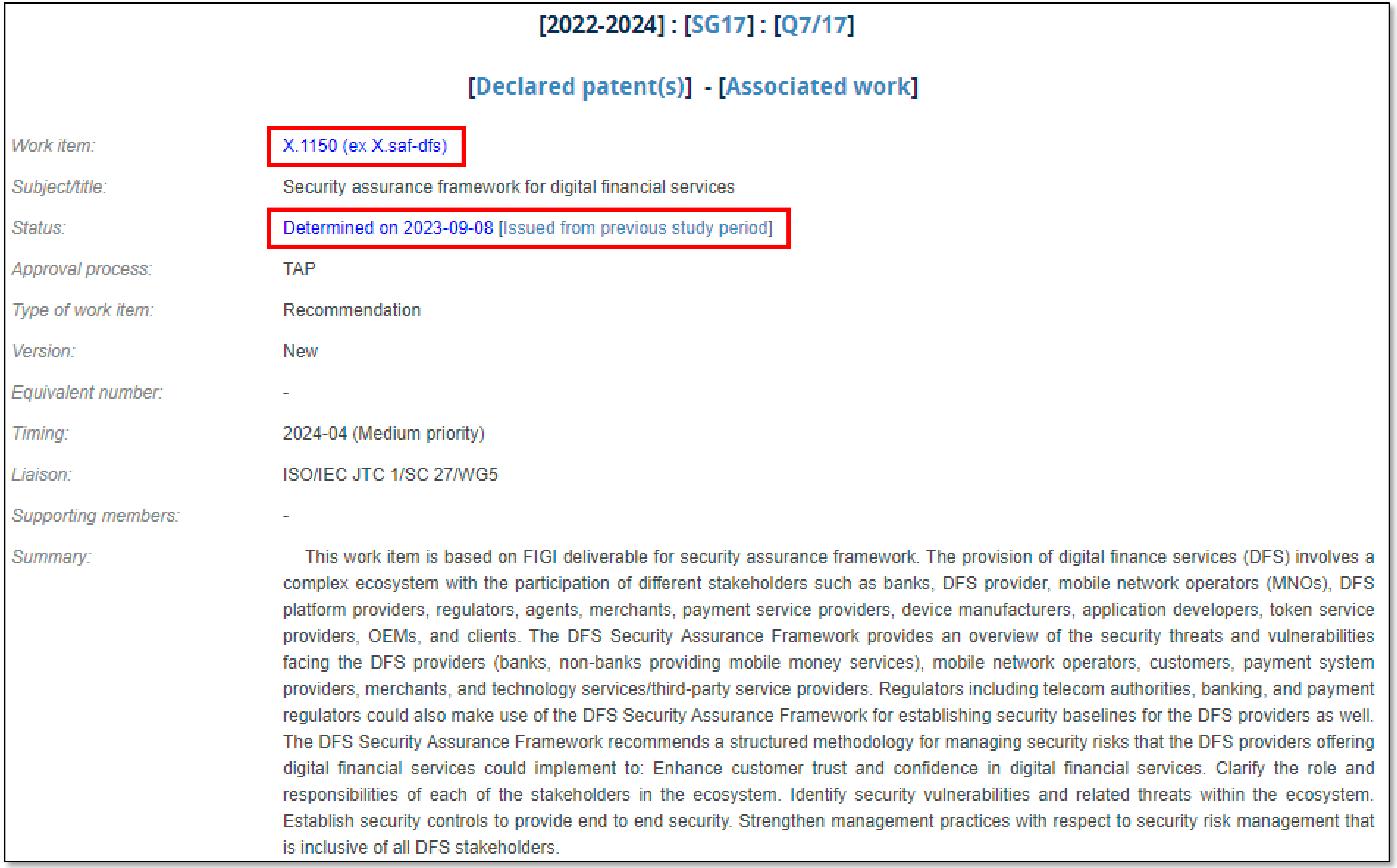
Contact: Junhyung Park
Soonchunhyang University
Korea (Republic of)
Tel: +82-41-530-1328
Email: junhyung.park@sch.ac.kr

Contact: Sungchae Park
Soonchunhyang University
Korea (Republic of)
Tel: +82-41-530-1328
Email: zoesc.park@sch.ac.kr

Abstract: This TD provides the 4th revised text for X.saf-dfs: Security assurance framework for digital financial services (for determination).

This TD provides the 4th revised text for X.saf-dfs: Security assurance framework for digital financial services, based on C361 and TSB edits(TD1285), at August/September 2023 SG17 Meeting in Korea.

Security assurance framework for digital financial services

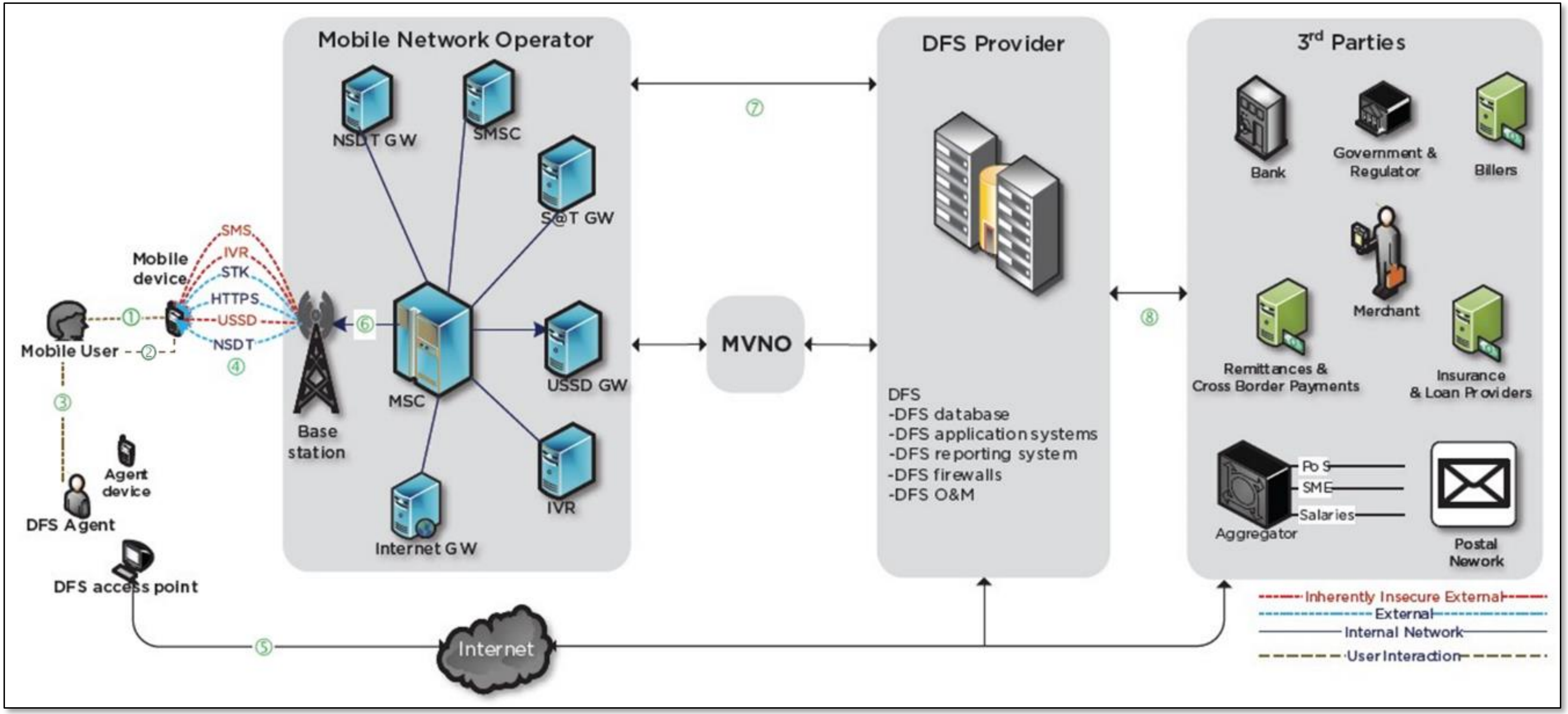


[2022-2024] : [SG17] : [Q7/17]

[Declared patent(s)] - [Associated work]

Work item:	X.1150 (ex X.saf-dfs)
Subject/title:	Security assurance framework for digital financial services
Status:	Determined on 2023-09-08 [Issued from previous study period]
Approval process:	TAP
Type of work item:	Recommendation
Version:	New
Equivalent number:	-
Timing:	2024-04 (Medium priority)
Liaison:	ISO/IEC JTC 1/SC 27/WG5
Supporting members:	-
Summary:	This work item is based on FIGI deliverable for security assurance framework. The provision of digital finance services (DFS) involves a complex ecosystem with the participation of different stakeholders such as banks, DFS provider, mobile network operators (MNOs), DFS platform providers, regulators, agents, merchants, payment service providers, device manufacturers, application developers, token service providers, OEMs, and clients. The DFS Security Assurance Framework provides an overview of the security threats and vulnerabilities facing the DFS providers (banks, non-banks providing mobile money services), mobile network operators, customers, payment system providers, merchants, and technology services/third-party service providers. Regulators including telecom authorities, banking, and payment regulators could also make use of the DFS Security Assurance Framework for establishing security baselines for the DFS providers as well. The DFS Security Assurance Framework recommends a structured methodology for managing security risks that the DFS providers offering digital financial services could implement to: Enhance customer trust and confidence in digital financial services. Clarify the role and responsibilities of each of the stakeholders in the ecosystem. Identify security vulnerabilities and related threats within the ecosystem. Establish security controls to provide end to end security. Strengthen management practices with respect to security risk management that is inclusive of all DFS stakeholders.

DFS Ecosystem



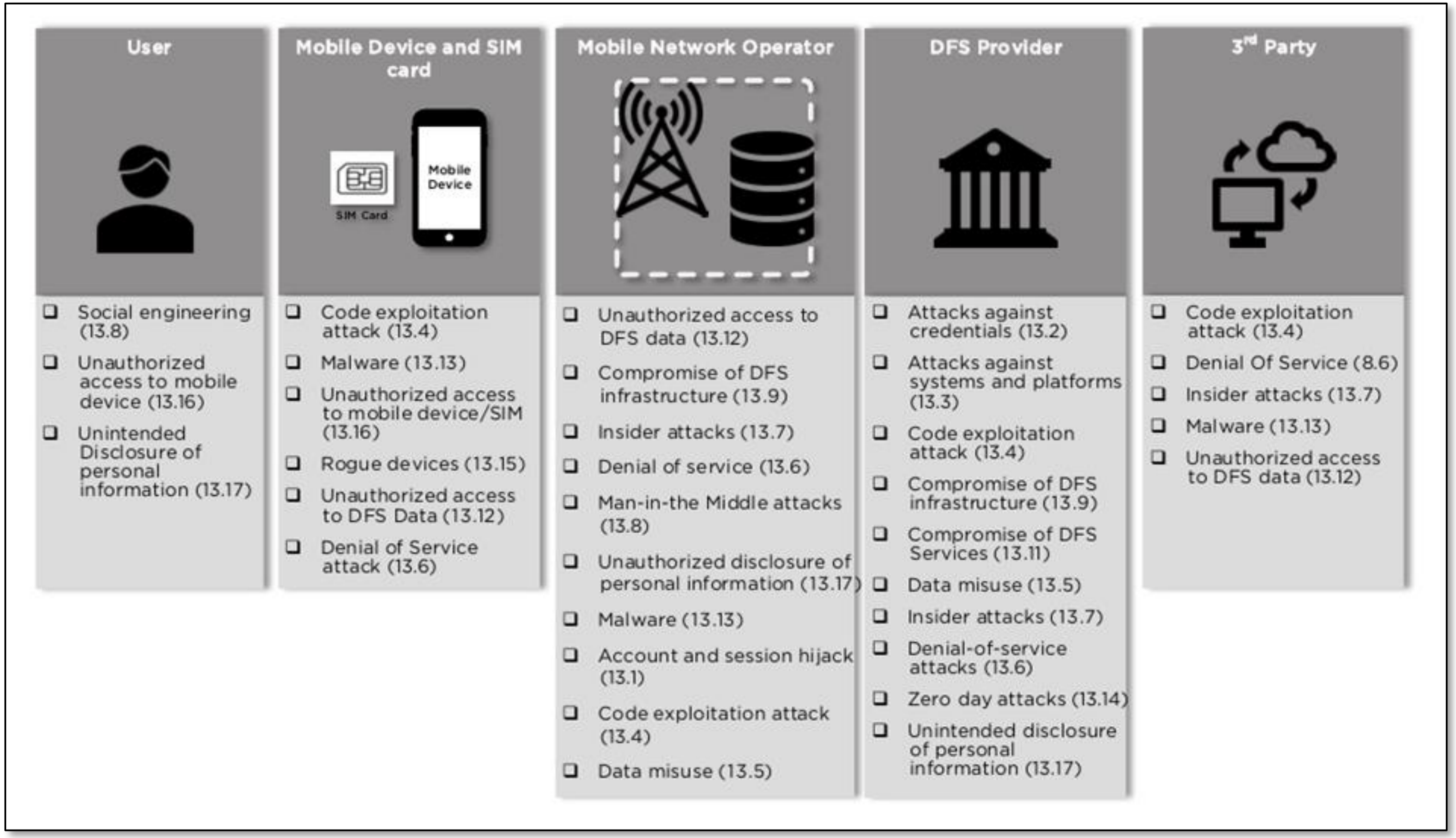
Source: ITU-T X.1150

DFS Ecosystem

Element	Characteristic	Example
User	• The target audience for a DFS service, who makes use of a mobile money application to interact with the service.	Customers
Mobile Devices	• The mobile device provides a plat form for deploying a mobile money application • It is the main channel through which the user	Smartphone, Feature phone, Mobile terminal
Mobile Network	• The carrier network provides transit connectivity for information originating at the user’s devices. • It is comprised of different nodes that enable communication to external providers and to DFS providers	USSD, IVR, STK, SMS
DFS Provider	• The DFS provider interfaces the application contents originating in mobile operator networks with the back-end financial providers and is used for administering the customers' information in a secure fashion, and allowing for services.	Bank, Card company, securities company
3rd party	• 3rd party allows for the interfacing between carrier-based mobile money systems and provide the basis for connecting with back-end financial networks such as the banking infrastructure	Fintech company, Payment company

Source: ITU-T X.1150

Security threats



User

- □ Social engineering (13.8)
- □ Unauthorized access to mobile device (13.16)
- □ Unintended Disclosure of personal information (13.17)

Mobile Device and SIM card

- □ Code exploitation attack (13.4)
- □ Malware (13.13)
- □ Unauthorized access to mobile device/SIM (13.16)
- □ Rogue devices (13.15)
- □ Unauthorized access to DFS Data (13.12)
- □ Denial of Service attack (13.6)

Mobile Network Operator

- □ Unauthorized access to DFS data (13.12)
- □ Compromise of DFS infrastructure (13.9)
- □ Insider attacks (13.7)
- □ Denial of service (13.6)
- □ Man-in-the Middle attacks (13.8)
- □ Unauthorized disclosure of personal information (13.17)
- □ Malware (13.13)
- □ Account and session hijack (13.1)
- □ Code exploitation attack (13.4)
- □ Data misuse (13.5)

DFS Provider

- □ Attacks against credentials (13.2)
- □ Attacks against systems and platforms (13.3)
- □ Code exploitation attack (13.4)
- □ Compromise of DFS infrastructure (13.9)
- □ Compromise of DFS Services (13.11)
- □ Data misuse (13.5)
- □ Insider attacks (13.7)
- □ Denial-of-service attacks (13.6)
- □ Zero day attacks (13.14)
- □ Unintended disclosure of personal information (13.17)

3rd Party

- □ Code exploitation attack (13.4)
- □ Denial Of Service (8.6)
- □ Insider attacks (13.7)
- □ Malware (13.13)
- □ Unauthorized access to DFS data (13.12)

Source: ITU-T X.1150

Security assurance framework for digital financial services

Security control

Element	Threat	Control
User	Social engineering	Customer to access and download DFS applications through official application release channels to mitigate the risk of running malware-infected apps.
	Unauthorized access to mobile device	Mobile devices should automatically lock after a period of inactivity, forcing device authentication to be performed to unlock the device before it is used for DFS transactions.
	Unintended disclosure of personal information	DFS providers should ensure that customer data in production environments is not used in test environments unless anonymized according to best practices.
Mobile Devices	Code exploitation attack	Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.
	Malware	Deploy security software products on all mobile devices, including antivirus, antispyware, and software authentication products to protect systems from current and evolving malicious software threats.
	Unauthorized access to mobile device/SIM	Mobile devices should automatically lock after a period of inactivity, forcing device authentication to be performed to unlock the device before it is used for DFS transactions.
	Rogue devices	MNOs should monitor devices used to connect to or otherwise access the DFS system to ensure that such devices have the latest patches, updated antivirus software, are scanned for rootkits and key loggers, and do not support network extenders.
	Unauthorized access to DFS data	Ensure all sensitive consumer data such as PINs and passwords are securely stored with strong encryption within the internal network and while at rest to mitigate internal threats against this data.
	Denial of Service attack	MNOs should take steps to ensure network high network availability to allow access to DFS services through USSD, SMS, and the Internet.

Source: ITU-T X.1150

Security assurance framework for digital financial services

Security control

Element	Threat	Control
Mobile Network Operator	Unauthorized access to DFS data	Ensure all sensitive consumer data such as PINs and passwords are securely stored with strong encryption with- in the internal network and while at rest to mitigate internal threats against this data.
	Compromise of DFS infrastructure	Use multi-factor or multi-model authentication for access to DFS accounts.
	Insider attacks	Limit, control, and monitor physical access to sensitive physical DFS infrastructure.
	Denial of service attack	MNOs should take steps to ensure network high network availability to allow access to DFS services through USSD, SMS, and the Internet.
	Man-in-the-Middle attacks	MNOs should do CLI analysis for calls/SMS to detect calls and SMS that may be spoofed to appear like DFS provider calls.
	Unauthorized disclosure of personal information	DFS providers should ensure that customer data in production environments is not used in test environments unless anonymized according to best practices.
	Malware	Deploy security software products on all mobile devices, including antivirus, antispyware, and software authentication products to protect systems from current and evolving malicious software threats.
	Account and session hijacking	Add session timeouts for USSD, SMS, application, and web access to DFS services.
	Code exploitation attack	Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.
	Data misuse	Ensure all sensitive consumer data such as PINs and passwords are encrypted, when traversing the network and while the data is at rest.

Source: ITU-T X.1150

Security control

Element	Threat	Control
DFS Provider	Attack against credentials	Enforce a maximum number of login attempts to DFS accounts for back-end users, merchants, agents and DFS customers on DFS systems (database, OS, application).
	Attack against system and platforms	Avoid direct access by external systems to the DFS back- end systems by setting up a DMZ that logically separates the DFS system from all other internal and external systems.
	Code exploitation attack	Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.
	Compromise of DFS infrastructure	Use multi-factor or multi-model authentication for access to DFS accounts.
	Compromise of DFS services	Use strong multi-factor authentication for user and third party provider access to DFS systems.
	Data misuse	Ensure all sensitive consumer data such as PINs and passwords are encrypted, when traversing the network and while the data is at rest.
	Insider attacks	Limit, control, and monitor physical access to sensitive physical DFS infrastructure.
	Denial of service attacks	Inbound internet traffic should be limited and continuously monitored.
	Zero day attack	MNOs along with DFS providers and payment services providers should patch systems to the latest versions provided by the vendor to defend against attacks that have been developed from older vulnerabilities.
	Unintended disclosure of personal information	DFS providers should ensure that customer data in production environments is not used in test environments unless anonymized according to best practices. Conversely, test data should not be migrated to the product.

Source: ITU-T X.1150

Security control

Element	Threat	Control
3rd party	Code exploitation attack	Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.
	Denial of service attack	Inbound internet traffic should be limited and continuously monitored.
	Insider attacks	Limit, control, and monitor physical access to sensitive physical DFS infrastructure.
	Malware	Deploy security software products on all mobile devices, including antivirus, antispyware, and software authentication products to protect systems from current and evolving malicious software threats.
	Unauthorized access to DFS data	DFS Providers/Merchants should consistently dispose of old devices.

Source: ITU-T X.1150

DFS Security assurance framework

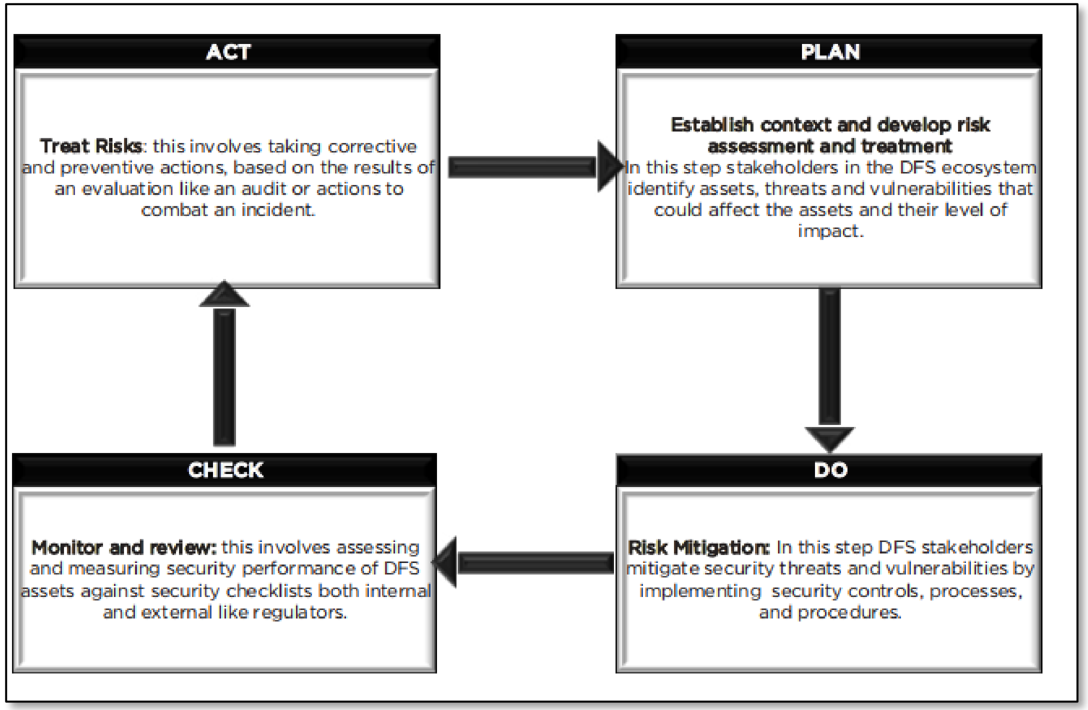
- DFS security assurance framework follows similar principle from:
  - ISO/IEC 27000
  - Payment Card Industry Data Security Standard(PCI-DSS) v 3.2
  - Payment Application Data Security Standard(PA-DSS)
  - NIST 800-53
  - Technical guidelines from Centre for Internet Security(CIS) controls V.7
  - OWSAP

- DFS security assurance framework consist of the following components:
  - A security risk assessment based on ISO/IEC 27005 (Clause 12)
  - Assessment of threat and vulnerabilities to the underlying stakeholders in DFS ecosystem.
  - Mitigation strategies based on the outcome of assessment of threats and vulnerabilities

- DFS security assurance framework identifies:
  - The various security threat to DFS assets
  - The related vulnerabilities that can be exploited by these threats
  - Security controls

Security risk management process

- In order to ensure a security model that is sustainable and continuously improves DFS security, this framework uses PDCA.
- Each figure shows PDCA step and high-level risk management process plan based on the PDCA.



ACT

Treat Risks: this involves taking corrective and preventive actions, based on the results of an evaluation like an audit or actions to combat an incident.

PLAN

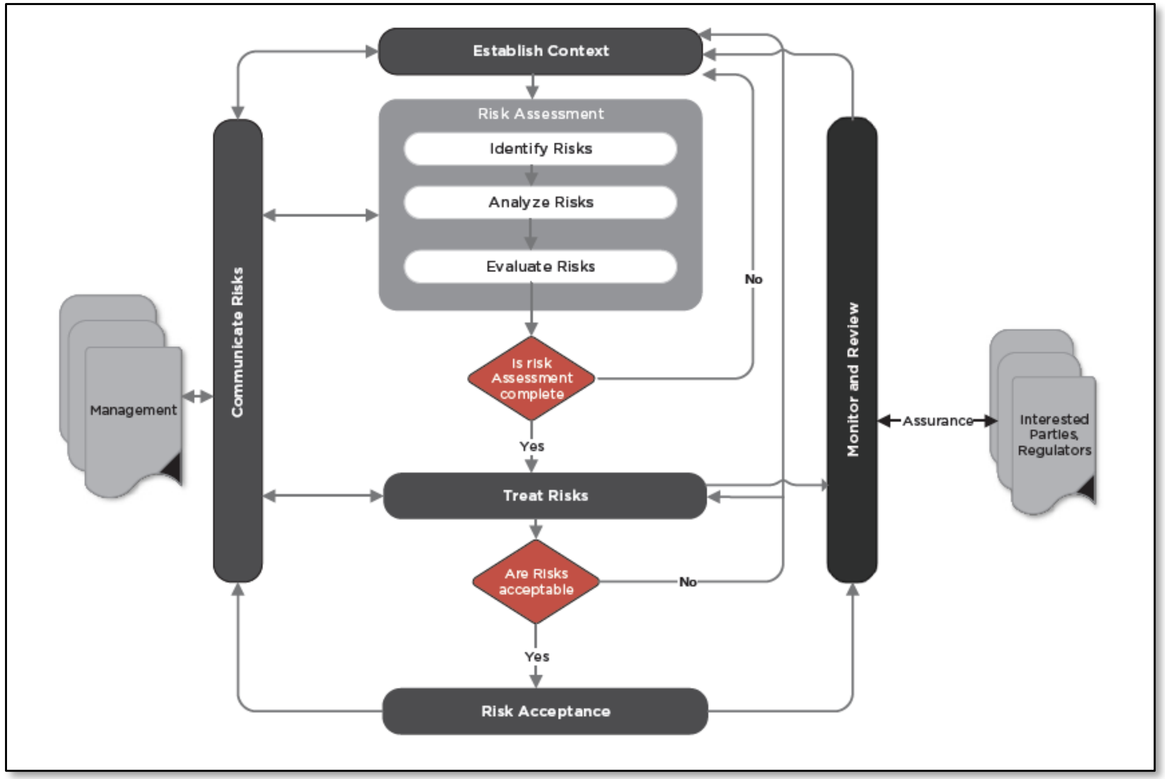
Establish context and develop risk assessment and treatment
In this step stakeholders in the DFS ecosystem identify assets, threats and vulnerabilities that could affect the assets and their level of impact.

CHECK

Monitor and review: this involves assessing and measuring security performance of DFS assets against security checklists both internal and external like regulators.

DO

Risk Mitigation: In this step DFS stakeholders mitigate security threats and vulnerabilities by implementing security controls, processes, and procedures.



DFS Security incident management

- Often even after relevant controls have been applied security incidents do occur, especially in financial services where attackers have a financial motive to evade systems, this causes system disruption, alteration or disclosure of data.

- Organizations and stakeholders offering and involved in digital financial services need to develop the right procedures, reporting, data collection, management responsibilities, legal protocols, and communications strategies that will allow the organization to successfully understand, manage, and recover from security incidents

- A security incident management plan defines consistent procedures to be followed for orderly, quick and effective reporting, response analysis, investigation and recovery from security incidents that compromise any of the ten security dimensions.

DFS Security incident management

No	DFS Security incident management
1	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management
2	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution
3	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles
4	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification
5	Assemble and maintain information on third party contact information to be used to report a security incident, such as law enforcement, relevant government departments, vendors and device manufactures
6	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities
7	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision-making, and incident responder’s technical capabilities using tools and data available to them
8	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures
9	Establish a disaster recovery system to prevent business disruption incidents such as natural disaster or cyber attacks to DFS systems
10	Respond to security incidents using a (SOAR) platform which collects threat-related data and automates threat responses

Source: ITU-T X.1150

Conclusion

Conclusion

- The financial industry is rapidly changing to the DFS format in line with the development of ICT technology.

- DFS is an industry that handles sensitive information along with customer and corporate assets.

- Due to the nature of the DFS industry, if a cyber threat occurs, it can cause great damage, so security must be considered a top priority.

- When considering security in DFS, you must consider not only confidentiality, integrity, and availability, but also transparency.

- In order to respond to cyber threats to DFS, a framework must be used to identify security threats that may occur in DFS and establish controls for them.

- We must constantly monitor new cyber threats and find ways to respond to them.

Thank you for your attention

SOON CHUN HYANG UNIVERSITY