A TOOLKIT FOR FINANCIAL SERVICE PROVIDERS

Building cyber resilience for digital financial inclusion and innovation

ACCION

UPDATED OCTOBER 2023

Acknowledgements

Mastercard Center for Inclusive Growth

In 2018, Mastercard and Accion launched a first-of-its kind partnership that united our global networks and resources to transform millions of underserved micro and small businesses, helping them fully participate in, and benefit from, the global economy. To solve this complex problem, the partnership combined digital transformation, fintech innovation, research, industry engagement, and talent philanthropy to get critical tools in the hands of small businesses and financial service providers who serve them. Through our partnership with the Mastercard Center for Inclusive Growth and with support from the Mastercard Impact Fund, we worked with nine financial service providers globally to guide and support their efforts to develop and adopt digital products and services to serve more small businesses more effectively. We are deeply grateful to our partners at Mastercard—including their dedicated leadership team, program staff, talent philanthropy volunteers, and communication teams—for their enthusiastic support for our shared mission to advance financial inclusion and inclusive growth.

About the Mastercard Center for Inclusive Growth

The **Mastercard Center for Inclusive Growth** advances equitable and sustainable economic growth and financial inclusion around the world. The Center leverages the company's core assets and competencies, including data insights, expertise and technology, while administering the philanthropic Mastercard Impact Fund, to produce independent research, scale global programs and empower a community of thinkers, leaders, and doers on the front of inclusive growth. For more information and to receive its latest insights, follow the Center on Twitter **@CNTR4growth**, **LinkedIn**, and **subscribe** to its newsletter.

.

Abbreviations and Acronyms

AI Artificial Intelligence

API Application Programming Interface

ATM Automated Teller Machine

DR Disaster Recovery

FSP Financial Services Provider

HSM Hardware Security Module

IAM Idendity and Access Management

IoT Internet of Things

MFA Multi-factor Authentication

MSE Micro and Small Enterprise

OTP One-Time Password

PAM Privileged Access Management

PIN Personal Identification Number

RPO Recovery Point Objective

RTO Recovery Time Objective

SIEM Security Information Event Management

Foreword

The disruption caused by the COVID-19 pandemic only accelerated the shift to digital, with a growing number of financial service providers using technology to streamline operations and deliver products and services to clients. Technology is meant to help FSPs, but one key element is often overlooked: the increasing exploitation of technological vulnerabilities that can cause real harm to FSPs and the clients they serve.

For low-income clients, the impact can be severe. In developing countries, it is often the customer who must prove and bear liability for losses in a cyberattack. The possibility of such an outcome decreases client trust and confidence in financial institutions and hinders progress toward financial inclusion.

IMF Managing Director Kristalina Georgieva addressed cybersecurity's role in advancing digital financial inclusion and innovation: "Beyond financial inclusion, growing cybersecurity risks threaten financial sector stability and integrity, as well as financial consumer protection. Cyberattacks also threaten digital financial service providers with potentially irreparable reputational damage that could lead to loss of market share and weaken incentives to innovate."[1]

Therefore, it is prudent for FSPs to ensure their digital transformations incorporate robust security and privacy measures when implementing innovative technology and solutions. If FSPs do not consider the inherent cyber risk, the likelihood of a successful digital transformation diminishes.

It may be tempting to hasten digitalization to capitalize on the opportunity. However, it is only by prioritizing cybersecurity and managing cyber risks that we can realize success and a better outcome, especially for those who are most vulnerable.

Prateek Shrivastava
Vice President, Digital
Accion Global Advisory Solutions

[1] IMF Managing Director Kristalina Georgieva's opening remarks at the Conference on Financial Inclusion and Cybersecurity, December 10, 2020

The Cyber Resilience Toolkit for Financial Service Providers

Cybersecurity refers to information and computer security, but also considers the protection of related information and telecommunications technologies, the data processed, and the infrastructure, products, and services depending on these technologies. As FSPs digitize, cybersecurity is critical to ensure that the organization's transformation remains future-proof, with proper governance, accountability, policies, and procedures in place and new norms of data protection and guidelines continually reviewed and considered.

Why is cybersecurity so important? Cybersecurity protects all categories of data from theft and damage, including sensitive data, personally identifiable information, protected personal information, intellectual property, and data and industry information systems. As FSPs' use of digital channels increases, so does the risk of exposing identity information. Neglecting cybersecurity can damage FSPs and incur severe costs.

- **Economic**: theft of intellectual property, corporate information, disruption in trading, and the cost of repairing damaged systems.
- **Reputational**: loss of consumer trust, loss of current and future customers to competitors, and poor media coverage.
- **Regulatory**: regulatory fines or sanctions as a result of cybercrimes.

The **Cyber Resilience Toolkit for Financial Service Providers** is a compendium of industry best practices and relevant highlights from a curated selection of industry publications. It also includes recommendations and tips from Accion's experience. The purpose of the toolkit is to help FSPs around the globe understand how to effectively mitigate cyber risk and strengthen cybersecurity. This toolkit is organized into five modules, each containing practical guidance for FSPs implementing a cyber resilience action plan to protect their systems, data, and their underserved clients' best interests.

We hope this guide is helpful as you plan your cybersecurity strategy. It is intended to complement Accion's Digital Transformation Guide.

01 Build secure apps

Create mobile apps with security considerations.

02 Test regularly for breaches

Understand the testing process, capabilities, and remedial action required to protect your institution and clients.

03 Create a culture of cybersecurity awareness rooted in strong organizational design

Tips for building and sustaining a culture of cyber awareness and incident handling.

04 Build a resilient technology environment

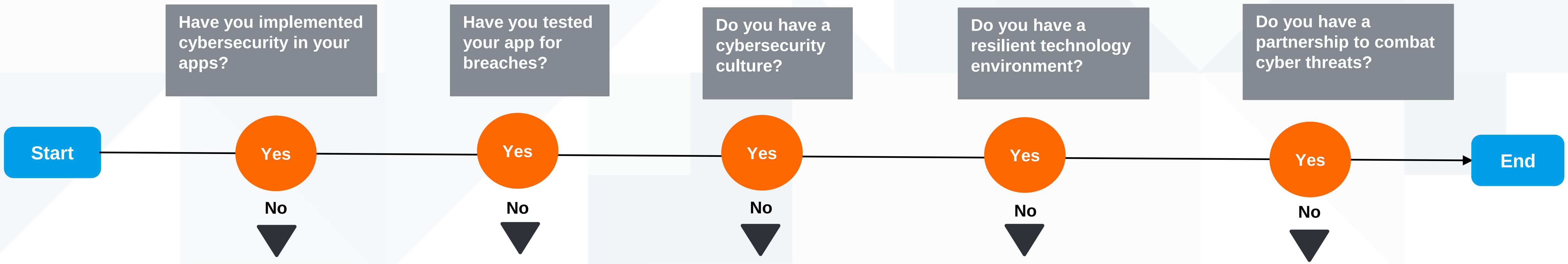
Learn how to build a robust infrastructure to proactively protect and sustain your institution and clients before, during, and after a cyber threat.

05 Strengthen cybersecurity with partnerships

Discover how understanding your capabilities and leveraging partnerships can reduce cyber risk and manage service delivery at minimal cost.

How to use the toolkit

This toolkit is divided into **five main modules**. Depending on the unique needs and requirements of your organization, you can explore it in sequence or choose to jump directly to specific modules.



Start

Have you implemented cybersecurity in your apps?

Yes

No

Have you tested your app for breaches?

Yes

No

Do you have a cybersecurity culture?

Yes

No

Do you have a resilient technology environment?

Yes

No

Do you have a partnership to combat cyber threats?

Yes

No

End

1.1 Implement cybersecurity considerations in product design

1.2 Implement building blocks for secure mobile apps

2.1 Create a successful testing process and procedure

2.2 Test regularly and protect your data

3.1 A cybersecurity culture drives proactiveness and preparedness

3.2 Tips for building a cybersecurity culture

3.3 Bridge the talent gap in cybersecurity

3.4 Assess the maturity of your cybersecurity culture

3.5 Avoid the common pitfalls

3.6 Design a high-level security architecture

3.7 Implement steps for a recovery plan

3.8 Recovery plan approach

4.1 Implement a cyber resilience strategy

4.2 Adopt a cybersecurity action plan

4.3 Identify cyber threats and protect your data

4.4 Maintain a continuous assessment of a balanced framework

5.1 What makes a cybersecurity partnership successful?

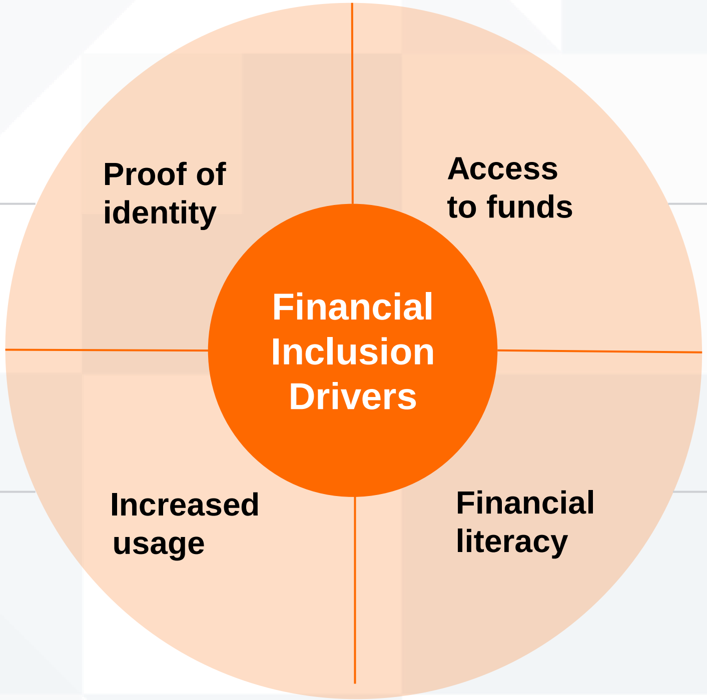
5.2 10 ways to test the cybersecurity partnership

Introduction

Technology as a driver for overcoming barriers to financial services at scale for the underserved

Implementing technology eliminates the common barriers that lead to the exclusion of millions of individuals from the formal financial system. Technology provides benefits that allow for the creation of new, non-traditional functions within financial service providers.[2]

To benefit from financial services, individuals must have a verifiable identity. Using technology such as biometrics to verify identities eases the onboarding process for new customers.



Proof of identity

Access to funds

Financial Inclusion Drivers

Increased usage

Financial literacy

While customers may have bank accounts, this does not equate to financial inclusion; customers only benefit when there are transactions and a flow of funds in the account. New digital payment options enable the flow of funds while providing customers convenient access to their accounts.

Financial inclusion involves using tools and resources that improve people's daily lives. Mobile-enabled solutions and access to digital channels drive the usage of digital financial services.

Clients do not always understand financial products offered by FSPs or the benefits and choices they can exercise Technology provides the capability to help customers understand this information. It also helps to deliver simple and easy-to-use products.

Technology offers FSPs unlimited potential to drive and overcome barriers to financial inclusion.

The use of technology in FSPs has led to the creation of new, non-traditional functions:

- **CLIENT ACCESS PROTECTION**
- **DATA PROTECTION**
- **CYBERSECURITY**
- **IDENTITY PROTECTION**
- **FRAUD DETECTION**

There is an increasing need for FSPs to build cyber resilience for financial inclusion and innovation.

[2] Adapted. Davis, C. (2021, March 30). *Driving purpose and profit through financial inclusion.* Deloitte https://www2.deloitte.com/us/en/insights/industry/financial-services/purpose-through-inclusive-finance.html

Why does cybersecurity matter now for FSPs?

The worldwide damages of cybercrime are expected to reach **$6 trillion by the end of 2021** and are expected to grow 15 percent every year to reach **$10.5 trillion by 2025**, according to Cybercrime Magazine. This could represent the greatest transfer of economic wealth in history, with profits greater than the global trade of all major illegal drugs combined.[3]

The complexity of systems continues to grow exponentially, so grows the probability of successful cybersecurity breaches. The ability to recover organizational infrastructure and business operations in case of their full or partial compromise can be challenging and irreversible.

Many factors contribute to the cost of cybercrime, and this can be attributed to a poor focus on best cybersecurity practices. Lacking cybersecurity practices can damage FSPs in several ways and incur serious costs.

ECONOMIC COSTS

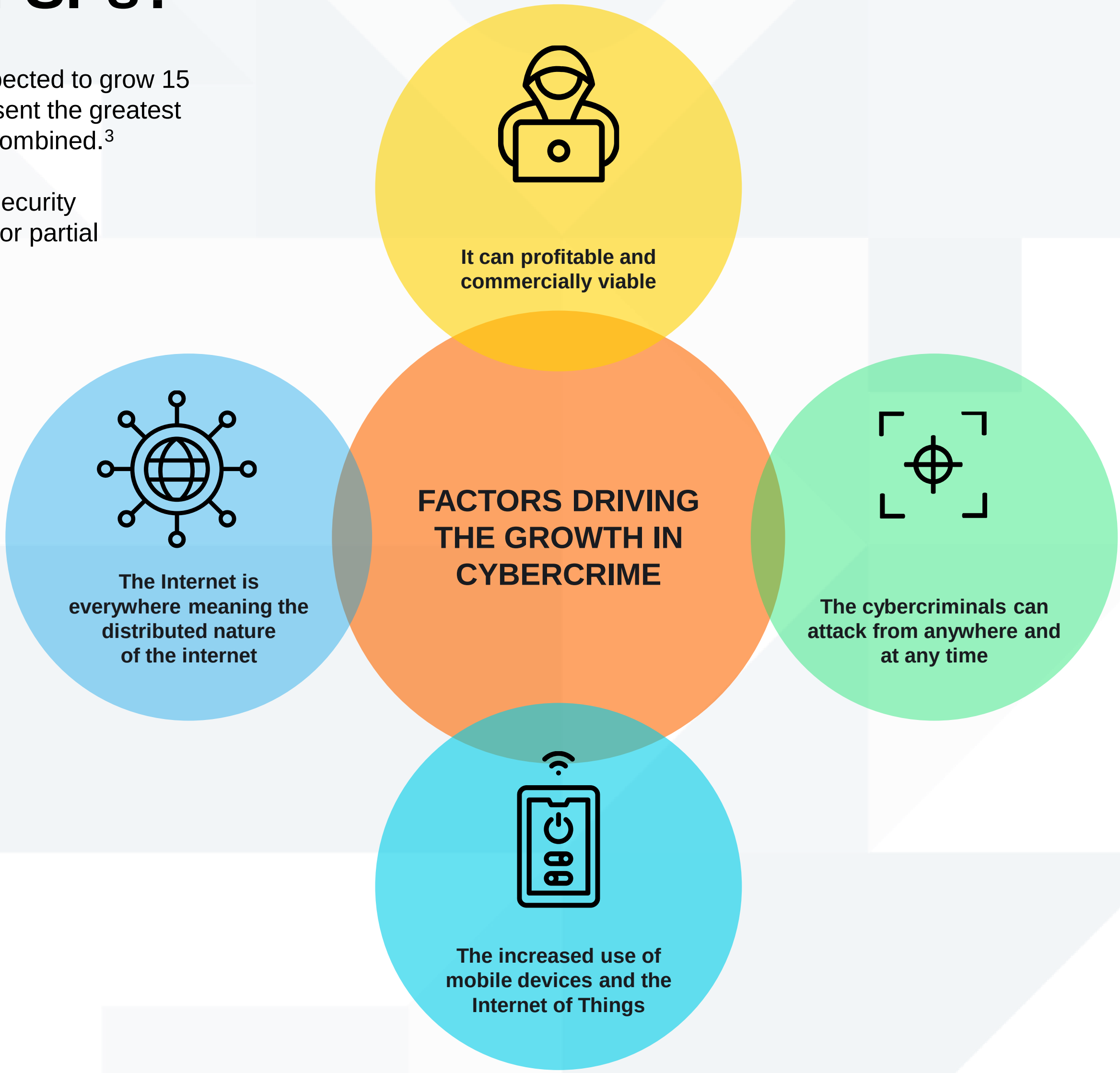
Theft of intellectual property, corporate information, disruption in trading, and the cost of repairing damaged systems

REPUTATIONAL COST

Loss of consumer trust, loss of current and future customers to competitors, and poor media coverage

REGULATORY COSTS

General Data Protection Regulation and other data breach laws mean that FSP organizations could suffer from regulatory fines or sanctions as a result of cybercrimes.



FACTORS DRIVING THE GROWTH IN CYBERCRIME

It can profitable and commercially viable

The Internet is everywhere meaning the distributed nature of the internet

The cybercriminals can attack from anywhere and at any time

The increased use of mobile devices and the Internet of Things

[3] Morgan, S. (2020, November 13). *Cybercrime to Cost the World $10.5 Trillion Annually by 2025.* Cybersecurity Ventures. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Changing customer experiences and trends and the impact on FSPs

COVID-19 and changing customer experiences and expectations have led to more FSPs building or acquiring mobile applications (apps). Payments and collections are increasingly done digitally, driving FSPs toward more self-service offerings. Mobile apps enable FSPs and clients to stay connected 24/7, enhance service quality, and create an important channel for cultivating customer loyalty. Increasing digital literacy among clients due to the use of social media and other mobile technology is also driving the trend toward mobile apps.

Why invest in mobile app development?[4]

Ability to reduce costs
Mobile transactions are much cheaper and faster than transactions at traditional bank branches and ATMs. The need for physical offices has decreased as the transactions can come from anywhere. Reduced operating and staff costs can be achieved without sacrificing customer service.

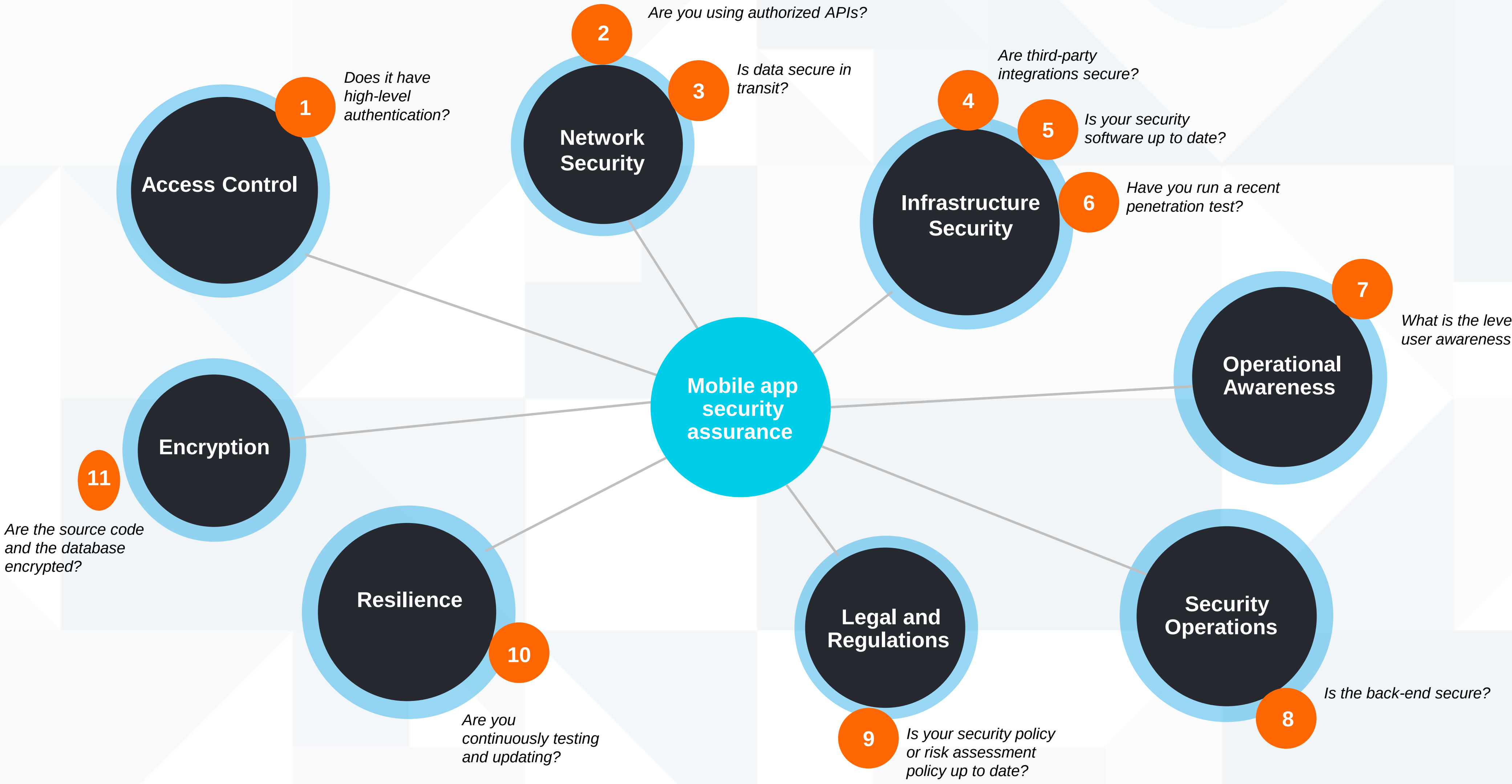
Ability to expand clientele
Consumers are attracted to mobile apps' convenience, round-the-clock accessibility, and various transactions performed via digital wallets, transfers, cashback, purchase discounts, vouchers, and coupons applicable to future transactions. Mobile apps can help capture that first digital-native generation of clients as they transition to adult life.

Ability to raise customer engagement and retention
Mobile apps empower FSPs to stay connected with clients conveniently 24/7, enhancing service quality and creating an important channel for cultivating customer loyalty. Push notifications can inform users about credit services, rates, new opportunities, and other activities. Round-the-clock accessibility to their account and transactions not only helps clients feel in control; if the service is easy to use, the more they will access it. Professional support provided via mobile apps also improves customer experience, promoting a higher customer retention rate.

Ability to increase revenues
Mobile apps are an additional way to market services that many customers perceive more favorably than direct sales at a branch. FSPs with mobile apps, and especially mobile-only FSPs, can partner with shops, cinemas, restaurants, and other businesses to offer discounts for their clients within mutually beneficial programs.

[4] Kholin, S. (2022, January 10). *Why and How to Build a Banking App*. Onix. https://onix-systems.com/blog/why-and-how-to-build-a-banking-app

Ensuring mobile app security[5]



Mobile app security assurance

Access Control

1 *Does it have high-level authentication?*

Network Security

2 *Are you using authorized APIs?*

3 *Is data secure in transit?*

Infrastructure Security

4 *Are third-party integrations secure?*

5 *Is your security software up to date?*

6 *Have you run a recent penetration test?*

Operational Awareness

7 *What is the level of user awareness ?*

Security Operations

8 *Is the back-end secure?*

Legal and Regulations

9 *Is your security policy or risk assessment policy up to date?*

Resilience

10 *Are you continuously testing and updating?*

Encryption

11 *Are the source code and the database encrypted?*

[5] Adapted. Vigliarolo, B. (2018, February 15). *How to Build a Secure Mobile App: 10 Tips.* TechRepublic. https://www.techrepublic.com/article/how-to-build-a-secure-mobile-app-10-tips. Hanumanthappa, M., Kumar, M., & Kumar, S. (2018, July 30). *Secure Mobile Application Development's Critical Issues and Challenges.* IJERT. https://www.ijert.org/research/secure-mobile-application-developments-critical-issues-and-challenges-IJERTCONV2IS02007.pdf

Contents

01 Build secure apps

02 Test regularly for breaches

03 Create a culture of cybersecurity awareness rooted in strong organizational design

04 Build a resilient technology environment

05 Strengthen cybersecurity with partnerships

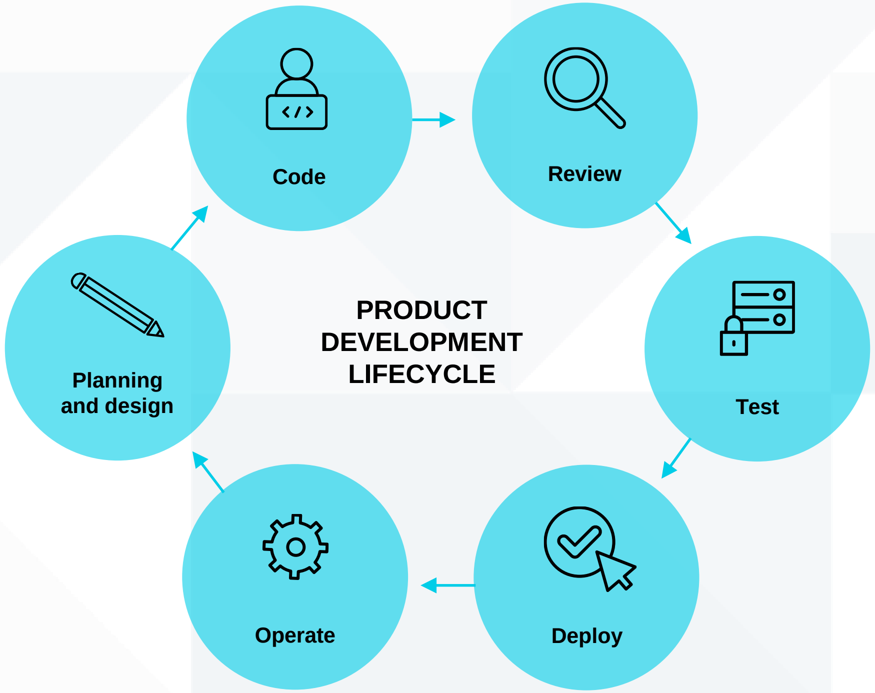
01

Build secure apps

1.1 Implement cybersecurity considerations in product design

Incorporating security in the early stages of product development results in **safer, more secure offerings and can spare companies the expense, hassle, and potential public embarrassment that accompanies retrofitting security**.[6]

BEST PRACTICES IN DEVSECOPS[7]



FSPs that are particularly small, largely serve MSEs, and unable to fully implement all recommendations can consider a gradual approach, outsourcing key skills or incorporating cybersecurity requirements into vendor procurement and management processes. Since MSEs may not be able to afford additional security devices like tokens, it is also imperative to design the system with the customer in mind.

PLANNING AND DESIGN

- Agile teams are aware of their security responsibilities from the outset; security champions are embedded in teams.
- Teams quickly model threats for all significant efforts.
- Backlog items are created, prioritized, and tracked to meet security and reliability requirements.
- Secure architecture designs are preapproved for implementation.

CODE

- Developers upgrade their skills in secure and resilient coding practices.
- Reusable coding patterns, components, and microservices are deployed to improve security and agility.

REVIEW

- Security is reviewed as part of every sprint and code release.
- Automated code analysis tools (Static Application Security Testing or SAST) are used to validate security.
- Senior developers with secure coding expertise conduct peer reviews.

TEST

- Security test cases are developed and automated by agile team members.
- Automated penetration testing (including Dynamic Application Security Testing or DAST and Interactive Security Testing or IAST) is performed as part of the developmental process.

DEPLOY

- Engineering teams work to progressively improve the path to production.
- Secure hosting environments "as code" ensure efficiency and repeatability.
- Strong encryption and authentication are built in.

OPERATE

- Real-time monitoring of app run time ensures potential security issues are identified.
- Host and network-based intrusion detection is implemented.
- Compliance validation and evidence gathering are automated.

[6] Curry, S. (2017, November 16). *Boards Should Take Responsibility for Cybersecurity. Here's How to Do It.* Harvard Business Review. https://hbr.org/2017/11/boards-should-take-responsibility-for-cybersecurity-heres-how-to-do-it

[7] Comella-Dorda, S., Kaplan, J., Lau, L. & McNamara, N. (2020, May 21). *Agile, reliable, secure, compliant IT: Fulfilling the promise of DevSecOps.* McKinsey Digital. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/agile-reliable-secure-compliant-it-fulfilling-the-promise-of-devsecops

1.2 Implement building blocks for secure mobile apps[8]

1

DATA PROTECTION

- Encrypt sensitive data
- Protect data sharing

2

AUTHORIZED ACCESS

- Build secure identification
- Authenticate via PIN, tokens, or passwords
- Create appropriate levels of authorization

3

RIGHT TALENT AND PLAN

- Recruit and use the right product development team
- Use a motivated implementation team
- Create well-defined roles and responsibilities

4

SOLUTION ARCHITECTURE

- Secure the application software

5

SECURITY MAINTAINANCE

- Log everything
- Analyze the logs
- Act accordingly
- Make improvements

6

TEST AND VALIDATE

- Organize safety-based testing
- Conduct penetration testing
- Conduct ethical hacking

7

SECURE INTEGRATION

- Check API security
- Use secure cloud services
- Use secure tokens for any information exchange

8

ZERO SECURITY BREACHES

- Integrate security in daily workflows

For FSPs that have already deployed a mobile app solution, it is possible to go through the building blocks to “harden” their apps against intrusions by eliminating vulnerabilities and increasing layers of security. This can be done step-by-step by prioritizing areas like access, data protection, and integrations. FSPs should also consider including frequently asked questions in the app for customers with low digital literacy.

[8] Adapted. Maropost. (2022, January 4). *8 Best Practices For Your Mobile App Security in 2022.* https://www.maropost.com/8-best-practices-for-your-mobile-app-security-in-2022/

02

Test regularly for breaches

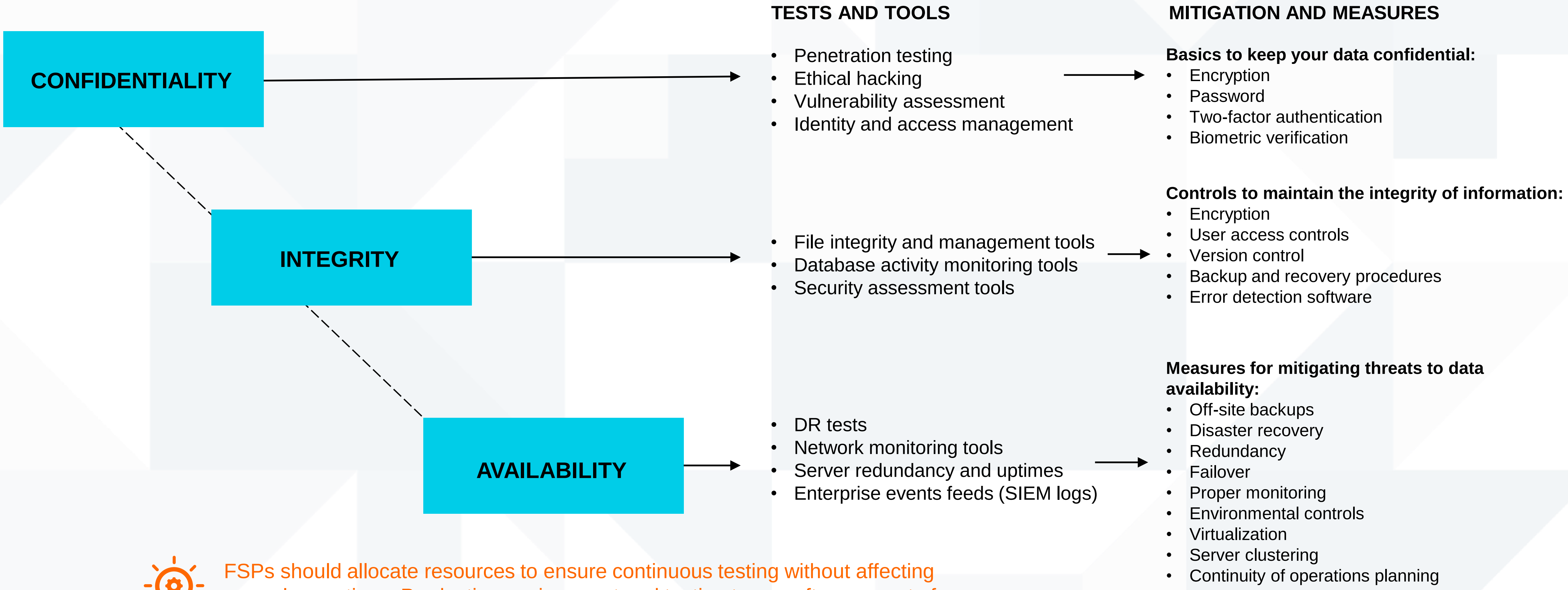
2.1 Create a successful testing process and procedure[9]

How is confidential information stored?	How is data integrity maintained?	How are the levels of authentication defined and enforced?	How are access levels maintained?	What are the availability standards maintained?	How easy is it to repudiate the data?
How is the FSP able to create a high level of **Confidentiality?** How is the FSP ensuring that the data confidentiality which focuses on the protection of bank client information is maintained? How secure is the exchange of data held by a client against third parties?	How does the organization measure and understand the level of **data Integrity?** How does the FSP maintain data integrity and assure the accuracy and completeness of data over its entire lifecycle? How can it be confirmed that data cannot be modified in an unauthorized or undetected manner?	What are the **authentication** processes and steps? What are the authentication processes in place and what needs to be improved? How does the authentication process verify that someone (or something) is, in fact, who (or what) it is declared to be? What are the ways of authentication in use? • Something the client is (e.g., biometric) • Something that they have (e.g., OTP or token) • Something they know (e.g., PIN or password)	**Authorization** levels and access verification: What are the existing policies for providing and specifying access rights/privileges to internal and external resources? Are authorization levels being put in place after a person has been identified and authenticated? How does the FSP determine what any person can then do on the system?	**Availability** of the mobile app and supporting systems. What are the agreed availability standards that asserts that a mobile app is available or accessible by an authorized client whenever it is needed?	Providing proof of the origin of data and the integrity of the financial data through **non-repudiation solutions.** What are we doing to ensure that non-repudiation is in place so that no party using the mobile app can deny that it sent or received a message via encryption and/or digital signatures or approved some information? How is it possible to ensure that clients cannot deny the transactions they initiated?

The chances of success are high if the organization assigns ownership and accountability for the testing process and procedure. Executive buy-in is essential to ensure that the people with the right authority are in charge of the process. Testing with clients is a good way to get feedback on the effectiveness of the controls and the user experience.

[9] Adapted. Islam, E., & Christoforides, C. (2019, November). *Fundamentals of cybersecurity and the Cyber Resilience Oversight Expectations (CROE).* European Central Bank. https://thedocs.worldbank.org/en/doc/880611573146903991-0130022019/original/Day1SessionIIIandIVECBEmranandConstantinos.pdf

2.2 Test regularly and protect your data using the CIA *(Confidentiality, Integrity, and Availability)* Model[10]



CONFIDENTIALITY

INTEGRITY

AVAILABILITY

TESTS AND TOOLS

- Penetration testing
- Ethical hacking
- Vulnerability assessment
- Identity and access management

- File integrity and management tools
- Database activity monitoring tools
- Security assessment tools

- DR tests
- Network monitoring tools
- Server redundancy and uptimes
- Enterprise events feeds (SIEM logs)

MITIGATION AND MEASURES

Basics to keep your data confidential:
- Encryption
- Password
- Two-factor authentication
- Biometric verification

Controls to maintain the integrity of information:
- Encryption
- User access controls
- Version control
- Backup and recovery procedures
- Error detection software

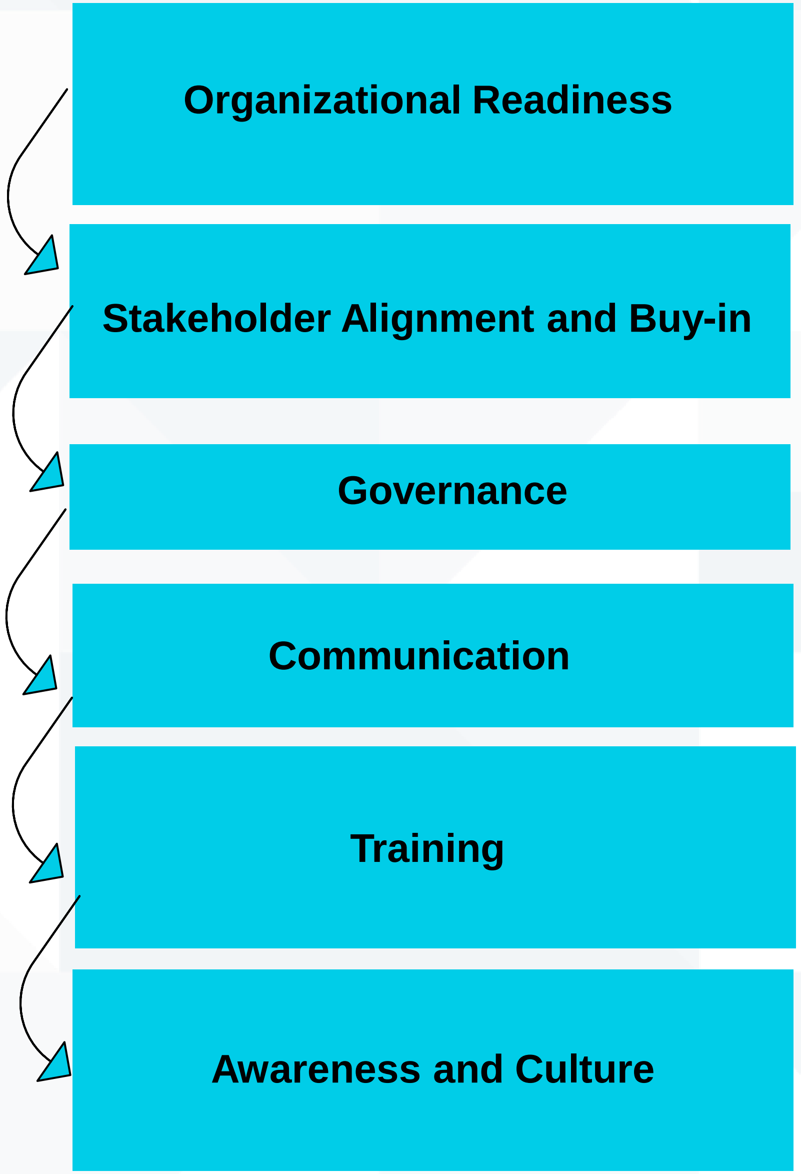
Measures for mitigating threats to data availability:
- Off-site backups
- Disaster recovery
- Redundancy
- Failover
- Proper monitoring
- Environmental controls
- Virtualization
- Server clustering
- Continuity of operations planning

FSPs should allocate resources to ensure continuous testing without affecting normal operations. Production environment and testing teams often compete for resources, requiring a policy document to help drive processes and procedures.

[10] Adapted. Komitas, S. (2022, October 5). *Addressing the Complexities of Cybersecurity at Fintech Enterprises.* ISACA. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/addressing-the-complexities-of-cybersecurity-at-fintech-enterprises

03

Create a culture of cybersecurity awareness rooted in strong organizational design



Organizational Readiness

Stakeholder Alignment and Buy-in

Governance

Communication

Training

Awareness and Culture

3.1 A cybersecurity culture drives proactiveness and preparedness

FSPs can achieve a higher degree of readiness to react to and recover from any cybersecurity risk or threat with a proactive approach.

FSPs can be proactive by accepting, adopting, and using new:

- Technology
- Processes
- Behavior/Culture
- Skill or talent
- Architecture
- Governance
- Ownership and Accountability

Awareness and training are characterized by:

- Attitudes
- Assumptions
- Norms
- Values
- Knowledge

FSPs should invest in training for MSE and other customers new to digital platforms to help them understand best practices in protecting their credentials and access. Digital adoption can be affected if customers do not trust new technologies. A good understanding of the customer segments helps tailor the messages appropriately for the audience.

3.2 Tips for building a cybersecurity culture[11]

The shift to remote work from COVID-19 has created a bigger cybersecurity risk for companies – nearly 60 percent of security professionals said working from home has made organizations more vulnerable to cyberattacks, and 60 percent of organizations have detected a moderate or severe uptick in cyberattacks since the start of the pandemic.

A cybersecurity culture is defined as a work environment in which every person is aware of cyber risks and is committed to reducing risks through their own behaviors and practices.

CHALLENGES TO CONSIDER

1. Budget
2. Security has a bad rap
3. Toxicity within cyber teams
4. Head of cybersecurity or Chief Information Security Officer (CISO) is poorly equipped
5. Inconsistent messaging creates confusion

BEST PRACTICES

Use your organization's current culture to create an appropriate cyber risk-aware culture

Outline a vision for a cyber risk-aware culture

Invest in the right security tools and develop security talent

Make security awareness training fun and rewarding

Involving all stakeholders, especially in small FSPs, can help create the organizational awareness needed to embed a cybersecurity culture in the fabric of the organization.

[11] Adapted. Deloitte.(2017). *Cultivating a cyber risk-aware culture. The Value of People.* https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fas-cultivating-a-cyber-risk-aware-culture.pdf

3.3 Bridge the talent gap in cybersecurity[12]

One of the challenges facing FSPs is the growing talent gap in cybersecurity. The gap between institutional capacity and what is required by the fast-evolving industry seems to be widening in most FSPs across the globe, as cybersecurity is a relatively newer field of expertise with a rapid pace of change in technology and the threat landscape.

Bridging the skills gap with automation solutions (artificial intelligence)

One way to tackle the skills gap challenge is with the use of high-tech automation solutions.

Security technology powered by artificial intelligence (AI) helps you to quickly detect and respond to sophisticated threats.

Automating manual processes and threat alerts can help fill critical voids. However, also look to your current resources, including existing teams, to fully address this issue.

New talent pools, new opportunities

One positive takeaway from the pandemic is the many career opportunities in the cybersecurity field.

As the concept of remote work becomes the norm and infrastructures become more distributed, the need for IT professionals that have timely security skills and knowledge will only grow.

The need for roles such as data scientists, cyber-savvy law enforcement staff, or threat hunters is only expected to rise.

Overcoming increased risk

With the pandemic creating a massive remote work shift and a consequent rise in cyber risk, finding individuals with cybersecurity skills is harder than ever.

Employers and employees can help overcome this challenge through training and certifications and bring greater organizational security amid uncertain times.

Increasing diversity by offering equal opportunities

Organizations are changing the hiring process and recruitment pool to take advantage of this potential employment pipeline.

Proactively encouraging the development of a diverse and inclusive talent pool requires leaders to understand the complex issues involved and demand that forward progress be made.

Attracting and retaining cybersecurity talent is expensive. FSPs should identify processes to automate to do more without creating large and unsustainable cybersecurity teams. Cybersecurity requires significant investment, in senior leadership attention, talent and skills, tools and systems, client education, and more. Related actions and investments must be planned and continuously assessed, ideally with board oversight.

[12] Adapted. Van Zadelhoff, M. (2017, May 4). *Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It.* Harvard Business Review. https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

3.4 Assess the maturity of your cybersecurity culture

DIMENSIONS[13]	STAGE 1: NASCENT	STAGE 2: DEVELOPING	STAGE 3: ADVANCED
ATTITUDES **Employee feelings and beliefs about security protocols and issues**	Employees believe that ensuring security protocols should be managed by IT	Employees believe they have a role in mitigating against security threats but that most issues will be managed by IT	Employees understand the importance of security protocols and see their role in upholding them
BEHAVIORS **Employee actions that impact security directly or indirectly**	Employees don't adhere to basic security precautions	Employees observe some security precautions but do not take active action to mitigate against them	Employees take action to actively mitigate against potential security threats
COGNITION **Employee understanding, knowledge, and awareness of security issues and activities**	Employees have limited awareness of potential security issues and what they can do to mitigate against them	Employees have some awareness of potential security issues	Employees are well informed of security issues
COMMUNICATION **How well communication channels promote a sense of belonging and offer support related to security issues and incident reporting**	Communication about security threats only happen when an incident has occurred	IT occasionally send out communication to staff about security threat prevention	Employees across the organization communicate regularly and proactively about security issues and mitigation
COMPLIANCE **Employee knowledge and support of security policies**	Employees do not comply with basic security policies	Employees comply with a majority of security policies	Employees comply with security policies nearly universally
NORMS **Employee knowledge and adherence to unwritten rules of conduct related to security**	Organizational norms around security awareness are non-existent and/or poorly understood by employees	Security norms may exist at an organizational level but may not be universally observed	Security norms are well documented, understood and observed by most staff
RESPONSIBILITIES **How employees perceive their role as a critical factor in helping or harming security**	Most employees don't believe they play an active role in preventing security breaches	Some employees believe they play an active role in preventing security breaches	All employees believe they play an active role in preventing security breaches

Independent assessment of the maturity of an organization's cybersecurity culture provides a balanced view that may offer greater benefits. For FSPs that cannot afford these external services, using internal risk teams with the necessary tools can meet the same objectives.

[13] Carpenter, P. (2021, May 27) *The Importance of a Strong Security Culture and How to Build One.* Forbes. https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/?sh=4e0fa8476d49

3.5 Avoid the common pitfalls[14]

DON'T WAIT FOR A BREACH TO HAPPEN.

If you wait for a cyberattack to happen, it is too late to act. Be proactive in implementing a cyber risk-aware culture. Culture changes can take a while to happen, so it is important to start early and monitor progress often.

ALIGN CULTURE OBJECTIVES TO CYBER RISK MANAGEMENT STRATEGY.

Your culture change objectives must be aligned with your organization's overall cyber risk management strategy. Ensure that culture change objectives include mitigation of common cyber risks, including operational impacts or denial of service.

TAILOR EFFORTS TO YOUR EMPLOYEES.

There is no one-size-fits-all solution when it comes to a cybersecurity culture. Segment employees and customize their engagement, communication, training, and assessment based on these attributes.

TAKE AN OMNICHANNEL APPROACH TO MESSAGING.

To be effective, a cyber risk culture campaign must leverage multiple channels of communication. Study how your employees leverage communication channels today and think about ways to creatively and effectively push content out to them.
Leverage behavioral principles such as nudges and the "fresh start" effect to time messages in a way that has maximal impact.

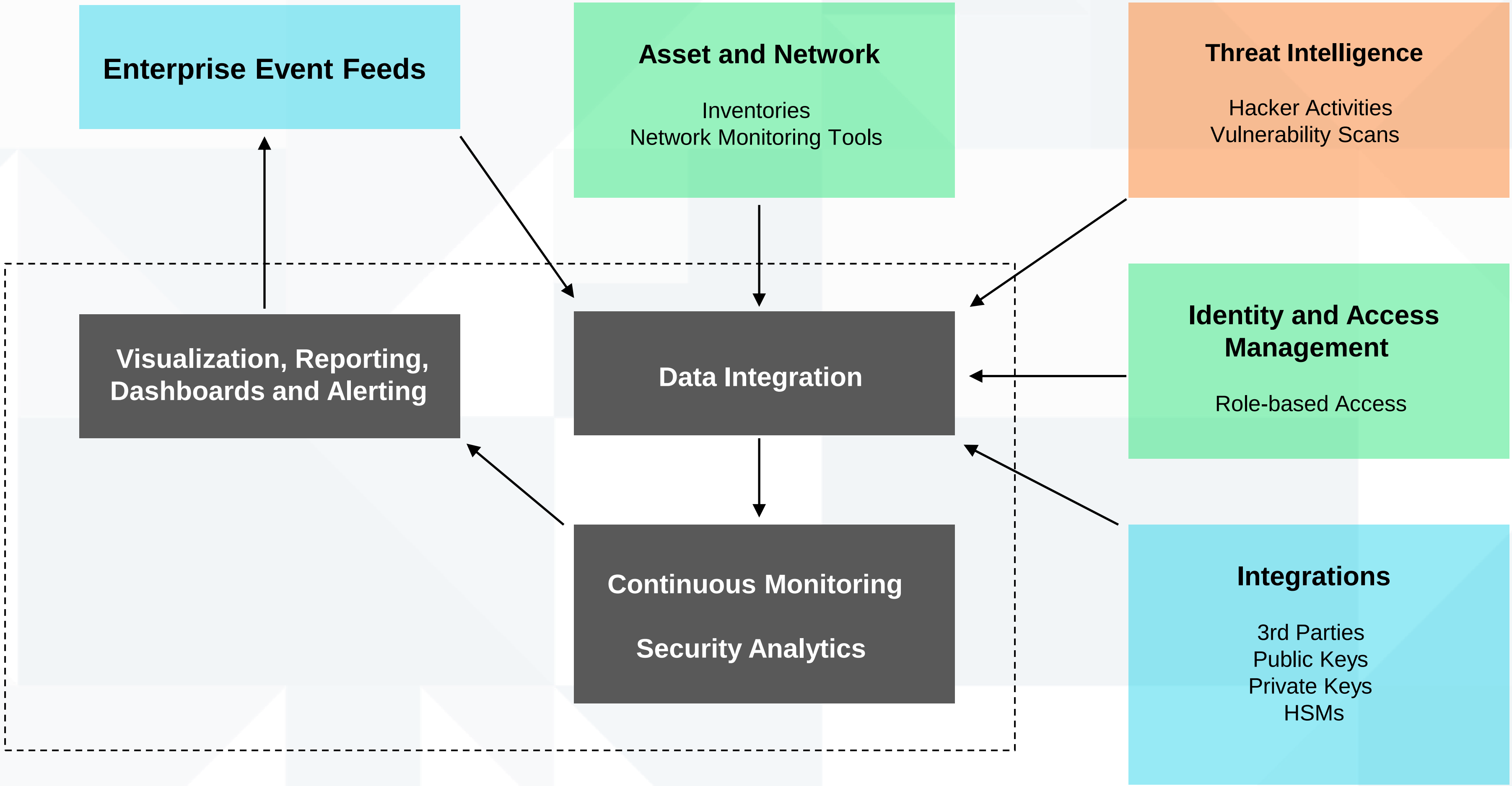
TEST AND EXPERIMENT.

Understand what works best by piloting initiatives with a smaller group prior to rolling out strategies with the entire organization. Test message content, timing, length, and channels to understand what works best when it comes to implementing new practices.

As FSPs digitize, security breaches are inevitable. FSPs must have the ability to reduce the impact on the business through their first line of defense, which is staff, not technology.

[14] Deloitte.(2017). *Cultivating a cyber risk-aware culture. The Value of People.* https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fas-cultivating-a-cyber-risk-aware-culture.pdf

3.6 Design a high-level security architecture[15]



Having a security architecture enables FSPs to produce a roadmap that can be used for budgeting, resource allocation, project planning, and coordination.

[15] Adapted. Dempsey, K., Chawla, N., Johnson, A., Johnston R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011, September). *Information Security.* National Institute of Standards and Technology. US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

3.6 Implement steps for a recovery plan[16]

IDENTIFY THE SCOPE OF THE DISASTER RECOVERY PLAN

The disaster recovery plan identifies exactly what the plan is to recover, where this information will be backed up, the underlying business policies, and the business impact of these decisions.

PROVIDE AN OVERVIEW OF OPERATIONS, GOVERNANCE AND ACCOUNTABILITY

Provide a general overview of operations, governance, accountability, and decision-makers, and identify who is responsible for each part of the disaster recovery plan.

IDENTIFY KEY SYSTEMS THAT MUST BE RECOVERED

Identify the key systems that must be recovered in the event of a disaster. Document the application profiles, priority systems, and system profiles. Note the:

- Recovery Point Objective (RPO) - the age of the data to restore.
- Recovery Time Objective (RTO) - the time needed to recover from a disaster.

PROVIDE AN INVENTORY PROFILE

Provide an inventory of the items that will need to be restored in the event of a disaster.

IDENTIFY NOTIFICATION & ACTIVATION PROCEDURES

Describe the actions that must be taken to detect and assess damages inflicted by a system disruption. Based on the assessment of the event, the Recovery Manager will activate the plan.

DESCRIBE THE PROCEDURES TO RECOVER THE SYSTEM AT BACKUP SITE

Document the procedures to recover the system at the alternate backup site. Perform each procedure in the sequence it is presented to maintain efficient operations.

TEST THE RECOVERY PLAN

Ensure the plan is tested and maintained so that it remains relevant and reliable if a disaster occurs. The document owner is responsible for ensuring that the plan accurately reflects recovery steps, contact details, and references that may change over time.

IDENTIFY ALTERNATIVE SITE RESOURCES

Outline the resources required at the alternative site (i.e. the site you will move to following a disaster) to ensure the operations can performed successfully.

IDENTIFY ACTIVITIES TO RESTORE OPERATIONS AT ORIGINAL OR NEW SITE

When the original site has been restored, operations at the alternate site must be returned. The goal is to provide a seamless transition of operations from the alternate site to the original site.

OUTLINE THE COMMUNICATION PROCESS

Describe the communication process in the event of a disaster situation. External communication is required to keep key stakeholders informed of project status, issues, and risks.

A business impact analysis is always recommended as a starting point to designing a recovery plan for FSPs. It helps define the KPIs of what success looks like when the recovery plan is fully operational.

[16] Adapted. Bartock, M., Cichonski, J., Souppaya, M., Smith, M. C., Witte, G. A., & Scarfone, K. (2016). *Guide for cybersecurity event recovery.* National Institute of Standards and Technology. US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

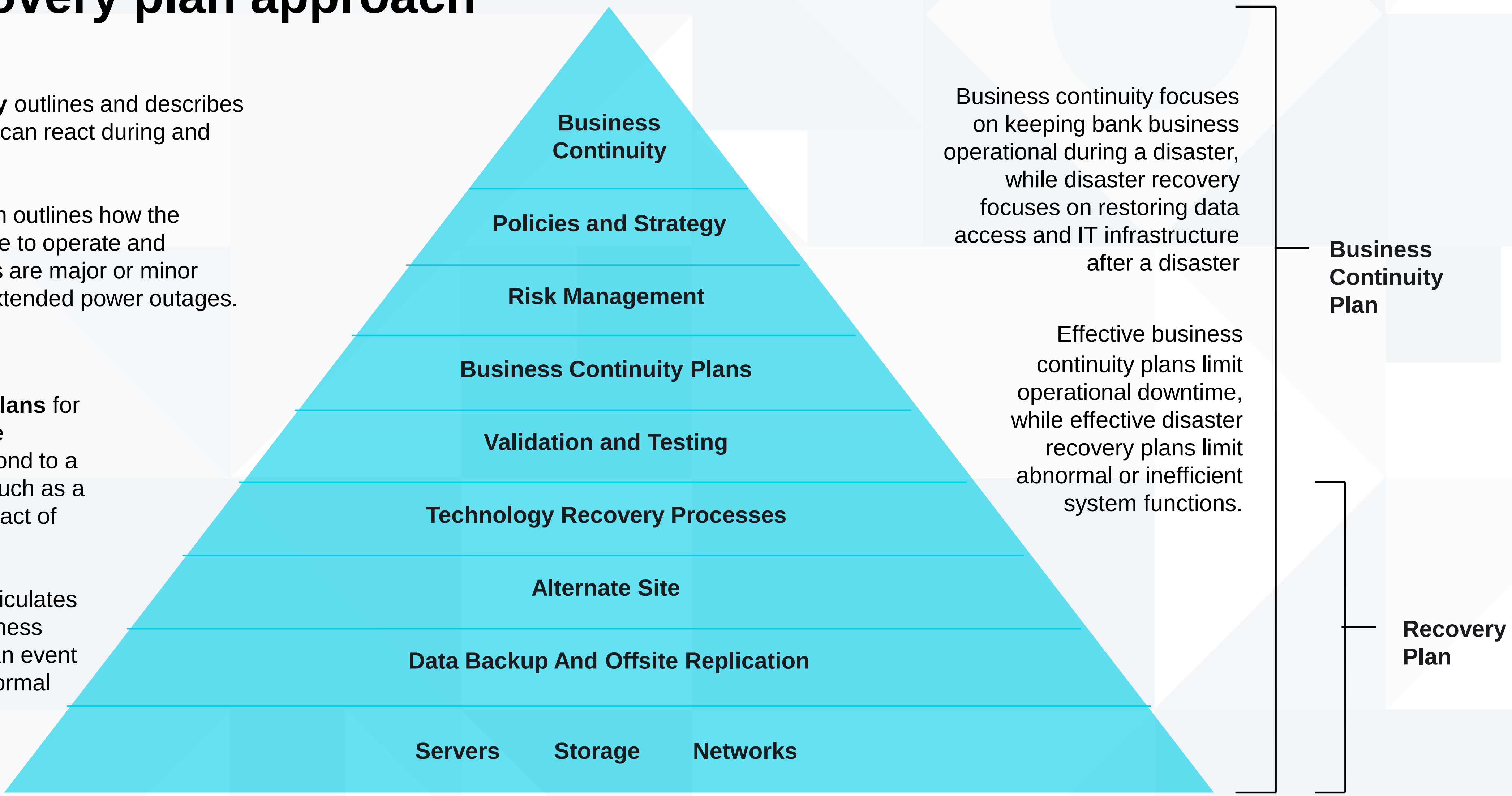
3.8 Recovery plan approach[17]

Business continuity outlines and describes how an organization can react during and following a disaster.

The contingency plan outlines how the business will continue to operate and whether interruptions are major or minor disasters, such as extended power outages.

Disaster recovery plans for FSPs outline how the business would respond to a catastrophic event, such as a natural disaster, fire, act of terror, or cybercrime.

Disaster recovery articulates the measures a business takes to respond to an event and return to safe, normal operation as quickly as possible.



Business Continuity

Policies and Strategy

Risk Management

Business Continuity Plans

Validation and Testing

Technology Recovery Processes

Alternate Site

Data Backup And Offsite Replication

Servers Storage Networks

Business continuity focuses on keeping bank business operational during a disaster, while disaster recovery focuses on restoring data access and IT infrastructure after a disaster

Effective business continuity plans limit operational downtime, while effective disaster recovery plans limit abnormal or inefficient system functions.

Business Continuity Plan

Recovery Plan

Recovery is mainly driven by people. It is important for FSPs to create organizational awareness of the various roles within the recovery process. Most recoveries fail because of a lack of adequate communication about who is supposed to do what, when, and how.

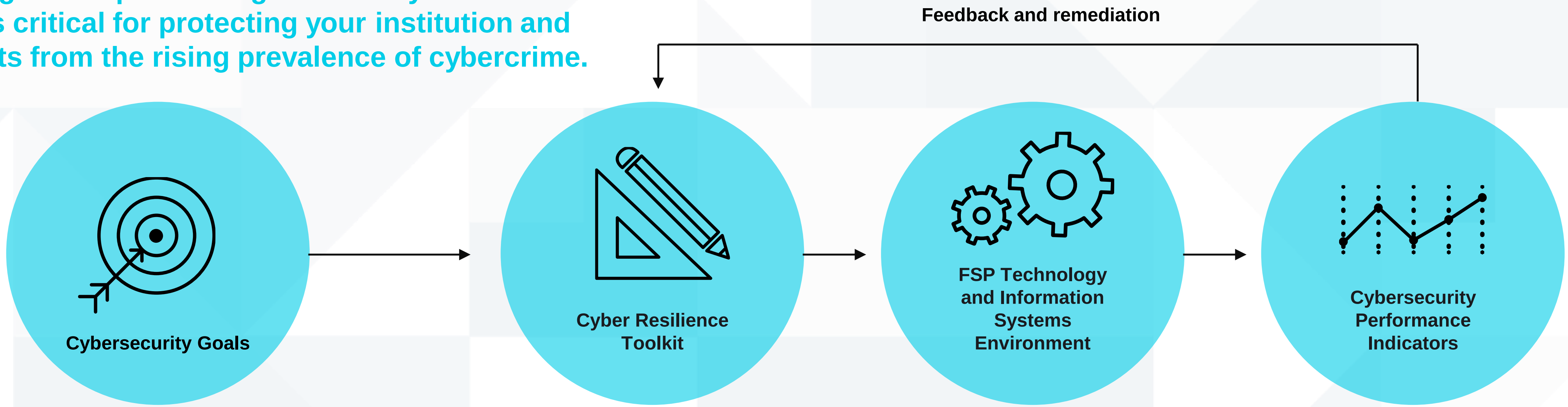
[17] Adapted. Bartock, M., Cichonski, J., Souppaya, M., Smith, M. C., Witte, G. A., & Scarfone, K. (2016). *Guide for cybersecurity event recovery.* National Institute of Standards and Technology. US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

04

Build a resilient technology environment

4.1 Implement a cyber resilience strategy[18]

Developing and implementing a sound cyber resilience strategy is critical for protecting your institution and your clients from the rising prevalence of cybercrime.



Feedback and remediation

Cybersecurity Goals

Cyber Resilience Toolkit

FSP Technology and Information Systems Environment

Cybersecurity Performance Indicators

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

1. Customer impact
2. Large increases (or decreases) in reported incidents
3. Total number of security incidents
4. Cost per incident
    - Direct costs
    - Indirect costs
    - Opportunity cost
5. Uptime
6. Regulatory Standards
7. Time to resolve

The cyber resilience strategy should be aligned with the business strategy and meet the expectations of the business impact analysis. Ownership and monitoring of the cyber resilience strategy's KPIs is important, as is managing the changes required for any remedial actions.

[18] Adapted. Bodeau, D., Graubart, R., McQuaid. R., & Woodil, J. (2018, September). *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring.* MITRE. https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

4.2 Adopt a cybersecurity action plan

Create a successful cybersecurity action plan using five critical pillars[19]

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment

Protect

- Asset Control
- Awareness Training
- Data Security
- Information Protection
- Processes and Procedures
- Protective Technology

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process
- Penetration Testing
- Ethical Hacking

Respond

- Resource Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Testing
- Communication
- Documentation

Maximize Protection, Minimize Risk.

Focus on deploying the key elements of a modern security approach to maximize protection and minimize risk.

Any action plan is dependent on the business process owners driving it. Identifying the business drivers allows the cybersecurity team and resources to focus on business priorities. This exercise is relatively straightforward and can be readily executed by small FSPs.

[19] Adapted. National Institute of Standards and Technology. US Department of Commerce (2013, November 12). *Cybersecurity Framework.* https://www.nist.gov/cyberframework

4.3 Identify cyber threats and protect your data[20]

Cybersecurity measures protect your data and help you maintain a competitive edge. Cyber threat actors may carry out attacks to disrupt your activities, steal data to sell, or give advantages to competitors.

COMMON CYBER THREATS

Phishing
Calls, texts, emails, or use of social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information.

Insider threat
Anyone who has access to an organization’s infrastructure and data can intentionally or unintentionally cause harm.

APPROACHES TO PROTECTING DATA

TRAIN EVERYONE WITH ACCESS TO INSTITUTIONAL INFORMATION

Train all staff, contractors, and others with access to institutional information to help them understand their roles in protecting the institution against cyber threats.

INSTALL SECURITY SOFTWARE AND TOOLS

Install security tools on systems and devices, such as firewalls and anti-virus software, that help protect institutional systems and networks from malware.

UPDATE AND PATCH DEVICES AND SOFTWARE

Update and patch devices and software to ensure systems are protected from security vulnerabilities (e.g. software bugs). Patching and updating software frequently will reduce the risks of cyber threats that can damage your institution’s systems and data.

IMPLEMENT ACCESS CONTROLS

Not everyone needs access to the same information. FSPs should practice the principle of least privilege to ensure that staff, contractors, and others with access to internal information only have the necessary privileges for their specific job. Granting excessive privileges puts institutions at a higher risk of data or privacy breaches.

All staff should have individual log-in credentials rather than using shared credentials for multiple people. Additionally, when staff change projects or leave the institution, be sure to revoke their privileges.

USE MULTI-FACTOR AUTHENTICATION

Multi-factor authentication uses two or more different methods of verifying identity (authentication factors).

BACK UP DATA

Backing up institutional data helps restore information systems after an attack, outage, or natural disaster. Ensure backups are stored on a device that is not directly connected to your primary network. This protects the backups from potential cyber attacks on primary systems (e.g. ransomware), remaining a path to restore if necessary. Test backups regularly.

FSPs that deploy automated solutions for common threats can deal with more complex and sophisticated attacks. Regularly testing backups is a regulatory requirement in most countries and provides added recovery capabilities. FSPs should provide ways of updating patches for customers like MSEs who might not have access all the time, which may create vulnerabilities on their devices.

[20] Canadian Centre for Cyber Security. *(2020 September). Security Considerations for Research and Development.* https://www.cyber.gc.ca/en/guidance/security-considerations-research-and-development-itsap00130

4.4 Maintain a continuous assessment of a balanced framework

A well-architected, risk-balanced framework is based on:[21]

Operational excellence
Ability to run and monitor systems to provide business value while continually improving support processes and procedures.

Security
Ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

Reliability
Ability to ensure systems can recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

Performance efficiency
Ability to use resources efficiently to meet system requirements and to maintain performance as demand changes and technologies evolve.

Cost optimization
Ability to run systems that provide business value at the lowest price point by minimizing or avoiding unnecessary costs.

Justifying investments in cybersecurity is always a challenge for FSPs. For most cyber risk practitioners, there is a need to closely examine the performance efficiency and reliability of technology solutions in the market. Service Level Agreements (SLAs) are critical for managing vendor relationships.

[21] EmergenceTek Group. (2021, October). *AWS Five Pillars of a Well-Architected Framework.* https://emergencetek.com/aws-five-pillars-of-a-well-architected-framework/

05

Strengthen cybersecurity with partnerships

5.1 What makes a cybersecurity partnership successful?

Strategic partnerships can be an effective strategy for securing systems and mitigating the risk of cyber-attacks.[22]

KEY BENEFITS TO CYBERSECURITY PARTNERSHIPS

- Addressing a cybersecurity talent and skills challenge
- Gaining access to cybersecurity experts as needed
- Easy access to information
- Freeing up time and resources of staff

BARRIERS TO EFFECTIVE COLLABORATION

- Trust and control of incident response
- Questions surrounding obligations regarding disclosure and exposure
- Evolving liability and regulatory landscape
- Challenges faced in cross-border investigation of cyber crime
- Data transfer restrictions that impede the ability to companies to respond to cyberthreats and incidents

FSPs can leverage partnerships to access cyber solutions without directly investing in on-premise acquisition and maintenance. Partnerships allow FSPs to focus on their core business and functions. Examples of partnerships include working with partners offering Security as a Service (SECaaS) such as vulnerability scanning, continuous monitoring, database security, and network security. SECaaS providers include Fortinet and RiskRecon.

[22] Six Degrees. (2020, November 4). *Four Ways Strategic Partnerships Improve Cyber Security.* https://www.6dg.co.uk/blog/cyber-security-strategic-partnerships/

5.2 10 ways to test cybersecurity partnerships[23]

1. Is the partner's solution a bolt-on or built-in integration?
2. Does the product roadmap synchronize to the primary vendor's releases?
3. Beware of partner-based solutions that require a new IAM or PAM platform.
4. Is the partnership efficient at producing production-level code at scale?
5. Is the additional partner going to help or hurt the organisation business?
6. Interview customer references running the partnership's solution.
7. What's the shared incident history of the partnership?
8. Third-party indemnification is a must-have.
9. Include random external security audits in the contract.
10. How secure are the DevOps cycles that partners are sharing to create products?

Successful partnerships need to have measurable parameters and specific outcomes. There should be an agreed method of collecting and analyzing data. Agreed-upon deliverables and timeframes must also be clearly communicated.

[23] VentureBeat. (2021, July). *10 ways to truth-test cybersecurity partnerships.* https://venturebeat.com/security/ciso-implementation-guide-10-ways-to-ensure-a-cybersecurity-partnership-will-work/

Learn more about protecting your institution from cybersecurity threats

Contact us

Gift Mahubo
Senior Director, Operations and Technology
gmahubo@accion.org

Diego Gaviria
Senior Manager, Digital Transformation
dgaviria@accion.org

ACCION