Building cyber resilience for digital financial inclusion and innovation
Acknowledgements

Mastercard Center for Inclusive Growth

In 2018, Mastercard and Accion launched a first-of-its kind partnership that unites 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 combines 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 are working 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.

This toolkit was authored by Gift Mahubo, Senior Director at Accion. The author is grateful to the many contributors to this toolkit, including Emma Morse, Prateek Shrivastava and Charlene Navarra.
Abbreviations and Acronyms

**AI** Artificial Intelligence
**API** Application Programming Interface
**ATM** Automated Teller Machine
**DR** Disaster Recovery
**FSP** Financial Service Provider
**HSM** Hardware Security Module
**IAM** Identity and Access Management
**IoT** Internet of Things

**MFA** Multi-factor Authentication
**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 prospect of losing even small amounts of money as a consequence of a cyberattack on their financial institution can be devastating. Particularly, as in most developing countries, when a cyber incident occurs, it is the customer who is liable for losses and carries the burden of proof. The possibility of such an outcome decreases client trust and confidence in financial institutions and hinders progress toward financial inclusion.

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.

Therefore, it is prudent for FSPs to properly shape the way we design, develop, and implement digital transformations to best manage and mitigate information security, privacy, and other risks, while still creating technology that helps people.

If FSPs carelessly implement technology to chase opportunities without considering the inherent cyber risk, the likelihood of realizing a successful digital transformation that can change lives and protect people diminishes.

By focusing on the opportunities along with the obligations to implement them in the right way, and by focusing on cybersecurity and managing cyber risks, we can achieve digital transformation and digital safety to ensure a better outcome for everyone.

Ultimately, it is not only information security practitioners but also business professionals who are accountable to the organizations they support, the customers they serve, and society, for achieving a safe and beneficial digital transformation.

Prateek Shrivastava
Vice President, Digital
Accion Global Advisory Solutions
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? Information theft is the most expensive and fastest-growing segment of cybercrime. 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 collates the learnings from Accion’s experience in helping FSPs around the globe understand how to effectively mitigate cyber risk and strengthen cybersecurity. This toolkit is organized into five main chapters, each containing practical guidance for FSPs implementing a cyber resilience action plan to better protect their systems, data, and their underserved clients’ best interest.

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, drawn from Accion’s deep expertise in change management.

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

Implementing technology can address key barriers that have historically led to the exclusion of millions of individuals from the formal financial system. With these benefits has come the creation of new, non-traditional functions within financial service providers.

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.

Financial inclusion requires tools and resources that are useful in people’s daily lives. Providing customers mobile-enabled solutions and access to digital channels can increase the usage of digital financial services.

Having a bank account does not mean inclusion; customers only benefit when there is a flow of funds from the account. Adopting new digital payment options enables this flow of funds while providing customers convenient access to their accounts.

Financial products are complex. Clients do not always understand their benefits or the choices they have. Using technology can help customers understand this information and 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

The increasing need for FSPs to mature new technology-related functions underscores the growing importance of building cyber resilience for continued progress on financial inclusion and innovation.
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% every year to reach $10.5 trillion by 2025 (Cybercrime Magazine, 2020). This could represent the greatest transfer of economic wealth in history, with profits greater than the global trade of all major illegal drugs combined.

While the complexity of systems grows 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 become a question of overall survivability for some organizations.

Many factors contribute to the cost of cybercrime and can be attributed to a poor focus on best cybersecurity practices. A lack of focus on cybersecurity can damage FSPs’ business in a range of ways, including:

**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**
- Increasing profitability and ease of commerce on the dark web
- The ability for cybercriminals to attack targets outside their jurisdiction makes policing extremely difficult
- The distributed nature of the internet
- The proliferation of mobile devices and the Internet of Things
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). Mobile apps empower FSPs to stay connected with clients 24/7, enhance service quality and create an important channel for cultivating customer loyalty.

Why invest in mobile app development?

Reduce costs
Fast mobile transactions are much cheaper than transactions at traditional bank branches and ATMs. Since they can be made from anywhere, the need for physical offices decreases. Operating costs and staff may be reduced without sacrificing customer service.

Expand your 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.

Raise customer engagement and retention
Mobile apps empower you 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.

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.
Ensuring mobile app security

1. Access Control: Do you have strong passwords or generators for all accounts?

2. Network Security: Are you using 2-step verification using OTP or tokens for all logins?

3. Infrastructure Security: Do you have a trustworthy IT vendor?

4. Encryption: Is your security software up to date?

5. Operational Awareness: Have you run a recent penetration test?

6. Legal and Regulations: Is your security policy or risk assessment policy up to date?

7. Security Operations: When was the last user awareness campaign done?

8. Security Operations: Is your data backed up either to cloud or physical media?

9. Disaster Recovery: When was DR last tested?

10. Disaster Recovery: Is the DR policy up to date?

11. Disaster Recovery: Is the encryption working properly?

12. Encryption: Have you changed WiFi passwords in the past 60 days?
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
Build secure apps
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.

**BEST PRACTICES IN DEVSECOPS**

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

**PLANNING AND DESIGN**

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

**CODE**

1. **Security is reviewed as part of every sprint and code release.**
2. **Automated code analysis tools (SAST\(^1\)) are used to validate security.**
3. **Senior developers with secure coding expertise conduct peer reviews.**

**TEST**

1. **Security test cases are developed and automated by agile team members.**
2. **Automated penetration testing (including DAST AND IAST\(^2\)) is performed as part of the developmental process.**

**DEPLOY**

1. **Engineering teams work to progressively improve the path to production.**
2. **Secure hosting environments “as code” ensure efficiency and repeatability.**
3. **Strong encryption and authentication are built in.**

**OPERATE**

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

---

1 Static application security testing
2 Dynamic application security testing and interactive application security testing

## Implement building blocks for secure mobile apps

<table>
<thead>
<tr>
<th>Step</th>
<th>Title</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PROTECT THE DATA</td>
<td>Encrypt sensitive data, Protect data sharing</td>
</tr>
<tr>
<td>2</td>
<td>PREVENT UNAUTHORIZED ACCESS</td>
<td>Build secure identification, Authenticate via PIN, tokens, or passwords, Create appropriate levels of authorization</td>
</tr>
<tr>
<td>3</td>
<td>RECRUIT THE RIGHT RESOURCES</td>
<td>Recruit and use the right product development team, Use a motivated implementation team, Create well-defined roles and responsibilities</td>
</tr>
<tr>
<td>4</td>
<td>CREATE THE RIGHT SOLUTION ARCHITECTURE</td>
<td>Secure the application software</td>
</tr>
<tr>
<td>5</td>
<td>CREATE AND MAINTAIN SECURITY LOGS</td>
<td>Log everything, Analyze the logs, Act accordingly, Make improvements</td>
</tr>
<tr>
<td>6</td>
<td>TEST YOUR SECURITY</td>
<td>Organize safety-based testing, Conduct penetration testing, Conduct ethical hacking</td>
</tr>
<tr>
<td>7</td>
<td>SECURE THE INTEGRATION CHANNELS</td>
<td>Check API security, Use secure cloud services, Use secure tokens for any information exchange</td>
</tr>
<tr>
<td>8</td>
<td>IMPLEMENT ZERO SECURITY BREACHES</td>
<td>Integrate security in daily workflows</td>
</tr>
</tbody>
</table>
Test regularly for breaches
## Create a successful testing process and procedure

<table>
<thead>
<tr>
<th>How is confidential information stored?</th>
<th>How is data integrity maintained?</th>
<th>How are the levels of authentication defined and enforced?</th>
<th>How are access levels maintained?</th>
<th>What are the availability standards maintained?</th>
<th>How easy is it to repudiate the data?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintaining a high level of Confidentiality of information</td>
<td>Measuring and understanding the level of data Integrity</td>
<td>Checking the ways and security of the Authentication processes and steps</td>
<td>Verifying Authorization levels and access</td>
<td>Setting and measuring Availability of the mobile app and supporting systems</td>
<td>Checking the levels of Non-repudiation solutions in place to provide proof of the origin of data and the integrity of the financial data</td>
</tr>
<tr>
<td>How are we ensuring that the data confidentiality which focuses on the protection of personal information is maintained?</td>
<td>How are we maintaining data integrity through maintaining and assuring the accuracy and completeness of data over its entire lifecycle?</td>
<td>What are the authentication processes and ways in place and what needs to be improved?</td>
<td>What are the existing policies and authorization levels providing and specifying access rights/privileges to internal and external resources?</td>
<td>What are the agreed availability standards that asserts that a mobile app is available or accessible by an authorized user whenever it is needed?</td>
<td>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?</td>
</tr>
<tr>
<td>How secure is the exchange of data held by a client with other users, against third parties?</td>
<td>How do we ensure that that data cannot be modified in an unauthorized or undetected manner?</td>
<td>How does the authentication process verify that someone (or something) is, in fact, who (or what) it is declared to be?</td>
<td>Are authorization levels being put in place after a person has been both identified and authenticated?</td>
<td>How are we determining what any person can then do on the system?</td>
<td>How is possible is to ensure that clients cannot deny the transactions they initiated?</td>
</tr>
</tbody>
</table>
Test regularly and protect your data using the CIA (Confidentiality, Integrity, and Availability) Model

Today’s FSPs face an incredible responsibility when it comes to protecting data. Whether it’s internal proprietary information or any type of data collected from customers, you could face substantial consequences in the event of a data breach. That’s why we need to have the right security controls in place to guard against cyberattacks and insider threats while also providing document security and always ensuring data availability.
Create a culture of cybersecurity awareness rooted in strong organizational design
A cybersecurity culture starts with proactiveness and preparedness

A proactive approach can help an organization achieve a higher degree of readiness to be able to react to any cybersecurity risk or threat.

Preparedness can be achieved through acceptance and adoption of new:

• Technology
• Processes
• Behavior/Culture
The shift to remote work from COVID-19 has created a bigger cybersecurity risk for companies – nearly 60% of security professionals said working from home has made organizations more vulnerable to cyberattacks, and 60% 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**

- Start with the C-suite and make security relatable
- Make it human-centric
- Invest in the right security tools and develop security talent
- Make security awareness training fun and rewarding
Bridge the talent gap in cybersecurity

One of the challenges facing FSPs has been 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 (artificial intelligence)

One way to tackle the skills gap challenge is with 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.
Assess the maturity of your cybersecurity culture

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

https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/?sh=4e0fa8476d49
Avoid the common pitfalls

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.

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.

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.

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.
Design a high-level security architecture

- Enterprise Event Feeds
- Asset and Network
  - Inventories
  - Network Monitoring Tools
- Threat Intelligence
  - Hacker Activities
  - Vulnerability Scans
- Identity and Access Management
  - Role-based Access
- Data Integration
- Continuous Monitoring
  - Security Analytics
- Visualization, Reporting, Dashboards and Alerting
- Integrations
  - 3rd Parties
  - Public Keys
  - Private Keys
  - HSMs
Implement steps for a recovery plan

IDENTIFY THE SCOPE OF YOUR DISASTER RECOVERY PLAN
The disaster recovery plan identifies exactly what you plan 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 and accountability, 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 you want 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.
**Recovery plan approach**

**Business continuity** outlines and describes how a business will proceed during and following a disaster. It provides contingency plans, outlining how the business will continue to operate whether it has to move to an alternate location. Business continuity planning may also consider smaller interruptions or minor disasters, such as extended power outages.

**Disaster recovery** refers to plans a business puts into place for responding to a catastrophic event, such as a natural disaster, fire, act of terror, or cybercrime. Disaster recovery involves the measures a business takes to respond to an event and return to safe, normal operation as quickly as possible.

Business continuity focuses on keeping 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.
Build a resilient technology environment
Implement a cyber resilience strategy

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

Cybersecurity Goals

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

Cyber Resilience Toolkit

FSP Technology and Information Systems Environment

Cybersecurity Performance Indicators

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
## Adopt a cybersecurity action plan

Create a successful cybersecurity action plan using five critical pillars:

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
</table>
| • Asset Management  
  • Business Environment  
  • Governance  
  • Risk Assessment | • Asset Control  
  • Awareness Training  
  • Data Security  
  • Information Protection  
  • Processes and Procedures  
  • Protective Technology | • Anomalies and events  
  • Security Continuous Monitoring  
  • Detection Process  
  • Penetration Testing  
  • Ethical Hacking | • Resource planning  
  • Communications  
  • Analysis  
  • Mitigation  
  • Improvements | • 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.
Identify cyber threats and protect your data

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.
Maintain a continuous assessment of a balanced framework

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

- **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.
Strengthen cybersecurity with partnerships
Why are successful partnerships critical for promoting cybersecurity?

Strategic partnerships can be an effective strategy for securing systems and mitigating the risk of cyber attack.

KEY BENEFITS TO CYBERSECURITY PARTNERSHIPS

- Addressing a cybersecurity 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
- Cross-border data transfer restrictions that impede the ability to companies to respond to cyberthreats and incidents
Use the 10 ways to truth-test cybersecurity partnerships

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 your 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.
10. How secure are the DevOps cycles that partners are sharing to create products?
Thank you.