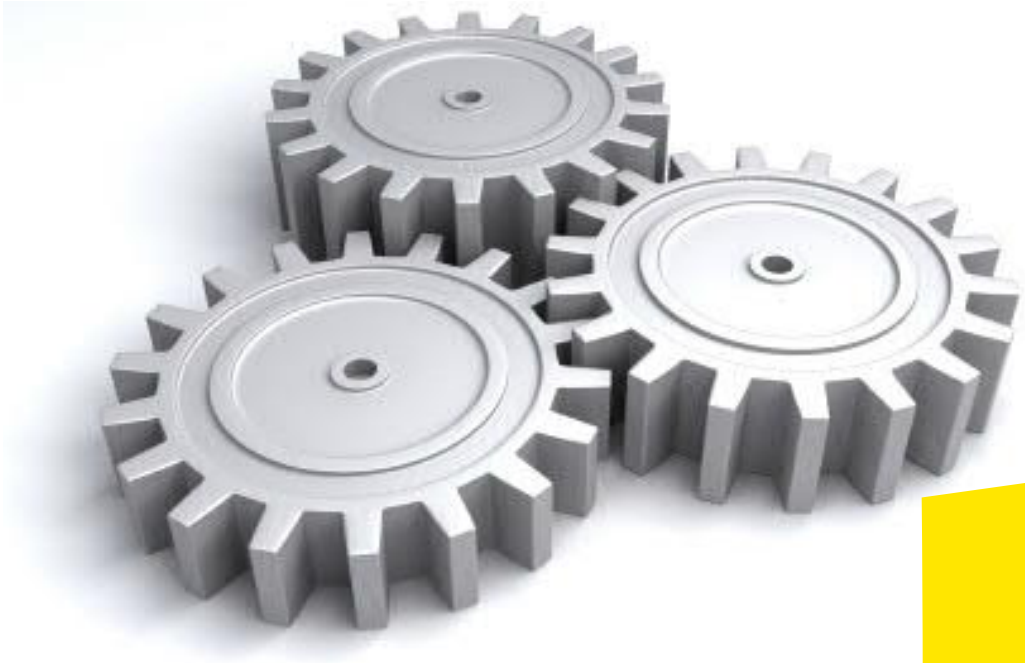


Impact of digital evolution on SACCOs

Benadatte Njoroge

July 2021

Objectives

- ✓ Why technology trends cannot be ignored
- ✓ Cybersecurity in digital evolution
- ✓ Cybersecurity considerations for SACCOs

Technology landscape

- The landscapes of technology and business are constantly changing and merging with each new innovation.
- Technology, is a key driver of innovation, and is at the heart of enabling business to evolve and maintain a commercial advantage.
- This shift has seen the role of technology within a business change from a support service to an integral player at the heart of operations, with the potential to be used to influence strategies and affect the shape of a business.

Technology trends

- Technology has become ubiquitous in business - technology is underpinning business models
- Technology is no longer just IT; enterprises are now digital and connected
- There is increase use of 3rd party providers
- Speed of innovation is outpacing risk management capabilities
- Technologies are only going to get more complicated and intricate as innovations advance

Technology stakeholders

- The business entity
- Customers
- Vendors
- 3rd parties
- Regulators

Technology trends

- Cloud computing
- Cybersecurity
- Artificial intelligence/ Machine learning
- Mobile computing
- Internet of things
- Quantum computing
- Robotic process automation
- Blockchain/ digital currency
- Wearable technology
- Virtual reality, Augmented reality, extended reality

Why adopt use of technology

- The COVID-19 pandemic forced many enterprises to reshape and rethink the way they conduct business, & emerging tech has helped organisations adapt quickly.
- Why adoption of emerging technology
  - Anticipated cost savings
  - Improved cybersecurity
  - Increased agility
  - The ability to reach new customers
  - Meet regulatory requirements
  - New revenue stream
  - Improved data privacy
  - Reputational value to your organization
  - A competitor’s successful implementation

Impact of adoption of technology

- Use of digital technologies to create new or modify existing processes, culture and customer experiences to create value.
  - Operational efficiency, improving customer experience, expanding into new markets, and managing risk
- Embracing change and adopting the appropriate technology to transform the business will contribute to companies surviving and staying ahead in a digital first world.

Example

- Example:
- Netflix vs Blockbuster
- Nokia vs Apple

Digital evolution in Saccos

Adoption of technology to support changing customer needs

- Use of mobile technology to support B2C transactions
- Adoption of core banking solutions to support digital transformation agenda
- Shift towards internet banking solutions
- Partnership with software vendors to provide solutions that offer competitive advantage

Cybersecurity in digital evolution

- The proliferation of connected devices coupled with today's vanishing perimeter and ever-changing threat landscape complicate an already complex environment for organizations to secure.

- Hackers are always looking for new ways to work through the gaps of all the controls and they are constantly innovating.

- The cybersecurity team has to support the business to confirm that adoption of a specific capability will not introduce risks to the business in as fast as the tech is being developed and deployed.

Cybersecurity trends

- Cybersecurity threats are here to stay

Cyber-attacks in Kenya up by half to hit 56m in three months

"A majority of the threats were malware attacks at 46 million, followed by web application attacks at 7.8 million while 2.2 million Distributed Denial of Service (DDos) threats were detected during the same period," the CA said in a statement.

According to a survey conducted by the Kenya National Bureau of Statistics (KNBS) and the CA, Kenya lost about Sh18 billion to cybercrime in 2016.

Cybersecurity trends cont'd

- Cybersecurity attacks
- The World Council of Credit Unions' (WOCCU), Technology and Innovation for Financial Inclusion (TIFI) project, funded through USAID's Cooperative Development Program (CDP), partnered with the Kenya Union of Savings and Credit Cooperatives (KUSCCO) and IRNet Coop Kenya (ICK) Limited to conduct an assessment of 18 savings and credit cooperatives (SACCOs) in Kenya to study their current cybersecurity strategies and experiences with cyber risks

  - five SACCOs reported having experienced a cyberattack in the past, with four out of this five reporting to have no system for transaction monitoring
  - eight cases where SACCOs did not have a digital transformation strategy;
  - five cases where there was no cybersecurity policy; and
  - nine cases where there was no budget allocated to cybersecurity priorities.

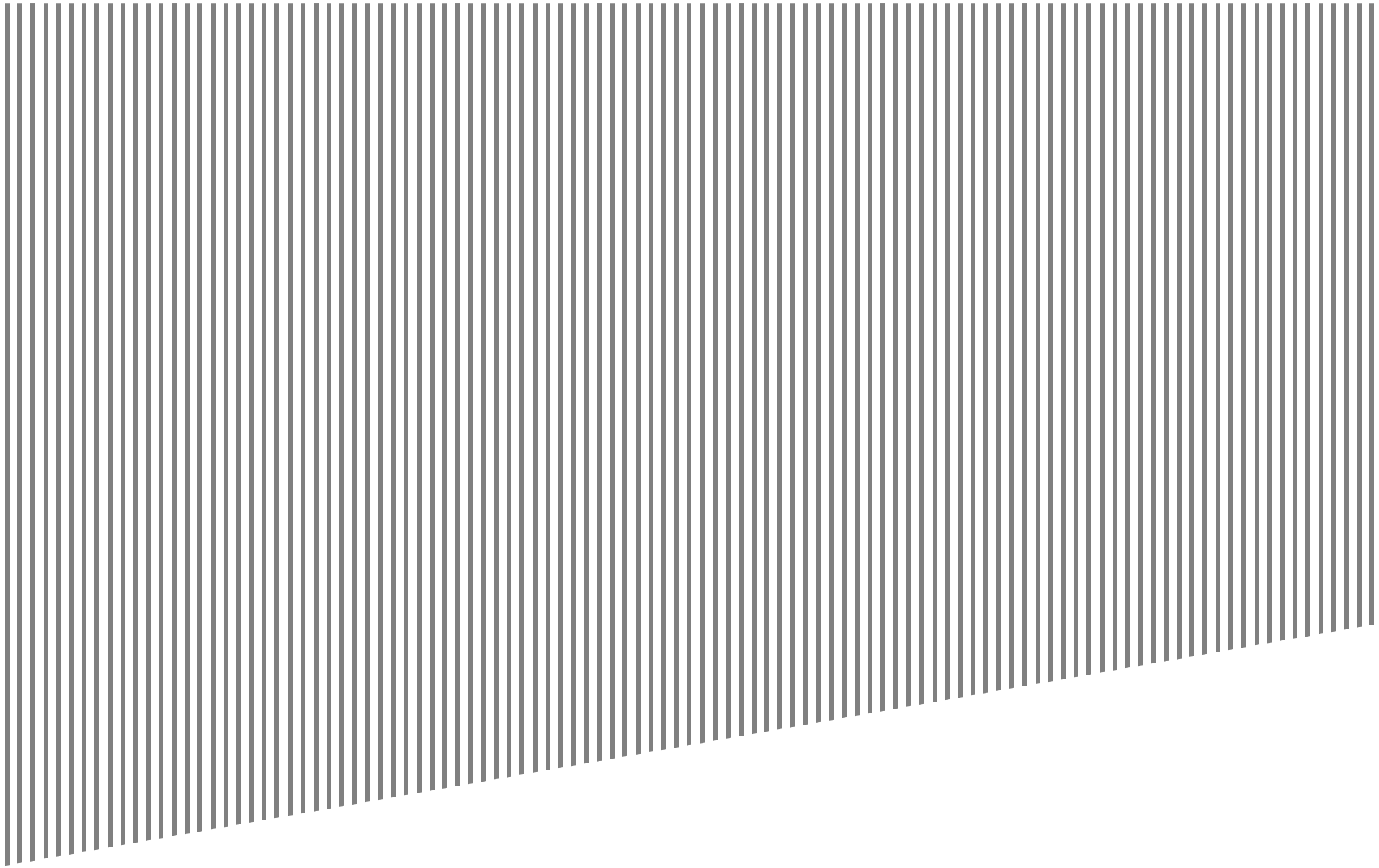
Cybersecurity trends cont’d

CBK issues cybersecurity guidelines to PSP after increase in attacks.

- According to the new guidelines, payment service providers are required to file cybersecurity reports with the industry regulator.
  - Governance
  - Assessment
  - Outsourcing
  - Awareness

SASRA risk management guidelines

- ICT risk management
  - Board and senior management oversight ; ICT strategy; ICT infrastructure; ICT management policies and procedures; Risk identification; Risk assessment ; Risk measurement ; Risk mitigation ; Internal control



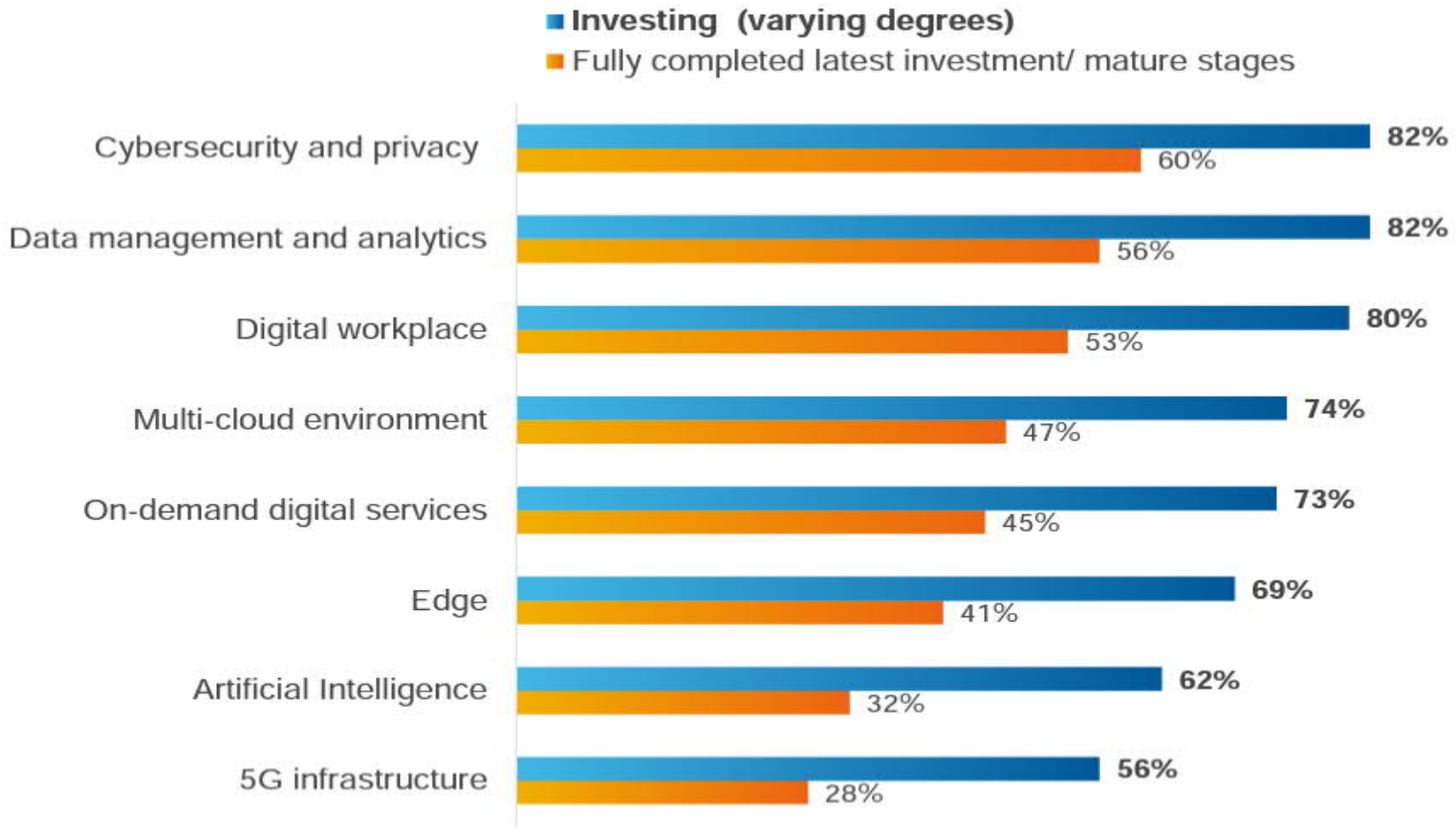
Cybersecurity in digital evolution

Digital Transformation Index 2020; 80% of businesses accelerated some of their programs which were:

- Strengthening cyber security defences
- Rolling out WFH/ remote working capabilities
- Reinventing how to deliver digital experiences to customers and employees

Cybersecurity in digital evolution

Current IT investments



DTI index 2020

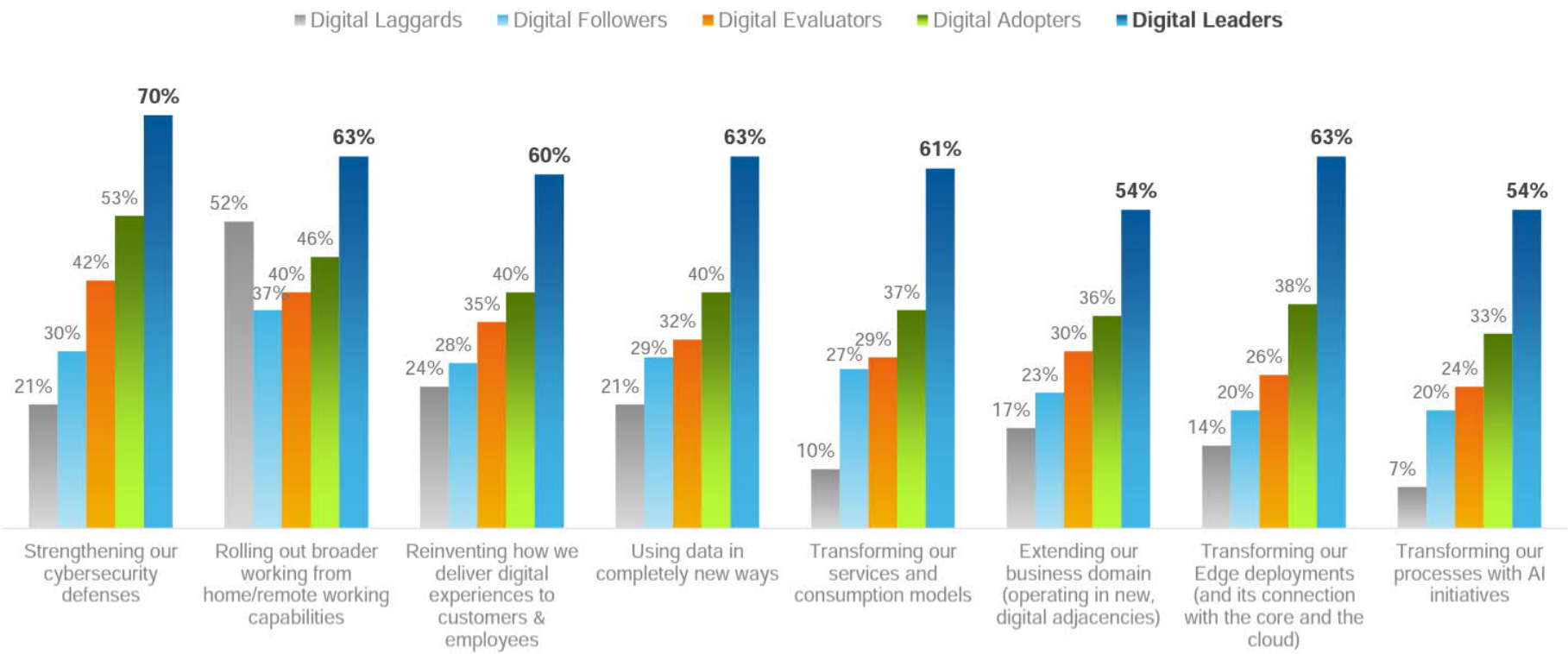
Cybersecurity in digital evolution

Planned investments over 1 – 3 years

DTI index 2020

Cybersecurity in digital evolution

Acceleration of key transformation programs



DTI index 2020

Cybersecurity in digital evolution

Why are organisations prioritising cyber initiatives?

- Organisations that are undergoing digital transformation, the whole digital enterprise becomes implicated, including the partner ecosystem.

- No organisation can totally safeguard themselves.
  - Cybersecurity is a continuous, always-on, proactive activity—not a task or a single point in a process
  - It’s a multi variant – involves people, process and technology

What does cybersecurity mean to you

"You may want to look into getting a better cybersecurity system. I don't think that sign will be enough."

Cybersecurity considerations for Saccos

Common cyber security pitfalls

- Lack of a cyber security policy – to give guidelines on baselines
- Sharing of passwords
- Using outdated technology
- Third parities with full access to your systems
- Lack of monitoring of user activities i.e. normal and privilege users

Cybersecurity considerations for Saccos

People, Process and Technology have to be in alignment for cyber initiatives to be effective

- People – All employees i.e. from new recruits to the board, need to realize how a cyberattack can erode trust in the organization.
  - Cultivate a cyber-resilient culture company-wide across your eco system

Cybersecurity considerations for Saccos

Processes provide an order of operations to follow.

- There should be a process in place to guide the cyber security initiatives.
- For example, what happens when a phishing attempt occurs?

Cybersecurity considerations for Saccos

- Cybersecurity response?

Cybersecurity considerations for Saccos

- Technology by itself will not secure your information.
  - Knowledge of what the tool does - what business problem is the tool solving
  - Know how of how to deploy it and customise it for your environment

Cybersecurity considerations for Saccos

Measures that can be adopted to mitigate cyber risks in Saccos:

- Development and enforcement of cyber security policy
- Privilege user accounts should be monitored – keep track of who has access to key assets
- Third parties and contractors should be monitored. (Third party risk management) – right to 3rd party audits clauses
- Implement segregation of duties
- Training and awareness – train staff on cyber security principles e.g. not to open links on emails
- Back up data

Cybersecurity considerations for Saccos

Measures that can be adopted to mitigate cyber risks in Saccos in the case of lack of resources depending on maturity levels:

- Out source/ Co-source – outsource full or partial functions.
  - Monitoring of resources can be outsourced to a mature organisation (people, process and technology)
  - An external party performing periodic assessments
  - Secondment of cybersecurity staff

- The outsourced model can be explored as you progressively build in house capabilities

Going forward

- Consideration of data privacy compliance after enactment of the Kenya Data Protection Act in 2019

https://www.youtube.com/watch?v=lO6O1_q3rFE

- User awareness/ education is of utmost importance: Cybersecurity is everyone's business
- Keeping abreast of emerging security trends and technologies
- Independent assessments should be periodic and should simulate IMPACT of the threats for better appreciation by stakeholders
- Risks need to be identified and addressed – tracking issue resolution
- Implementing the basics is more important than the latest solutions
- Cyber risk should be a standard agenda at the senior management level

.

Q&A

Questions?