SACCO CYBERSECURITY REPORT 2018
Demystifying Cybersecurity for Saccos
# Content

<table>
<thead>
<tr>
<th>01. Introduction</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highlights</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>02. Evolution and Impact of Saccos</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic Impact of Saccos in Kenya</td>
<td>6</td>
</tr>
<tr>
<td>Gross Domestic Product</td>
<td>6</td>
</tr>
<tr>
<td>Revenue Growth</td>
<td>6</td>
</tr>
<tr>
<td>Number of Employees</td>
<td>7</td>
</tr>
<tr>
<td>Growth in Number of Saccos</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>03. State of Cyber security in Saccos</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Budget</td>
<td>8</td>
</tr>
<tr>
<td>Cybersecurity Training</td>
<td>8</td>
</tr>
<tr>
<td>BYOD Usage</td>
<td>8</td>
</tr>
<tr>
<td>Cloud and IoT</td>
<td>8</td>
</tr>
<tr>
<td>Cybersecurity Management</td>
<td>9</td>
</tr>
<tr>
<td>Skill Gap</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>04. Threats due to digitization and Mobile usage</th>
<th>10</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>05. Server Vulnerabilities</th>
<th>11</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>06. Sacco Industry Challenges</th>
<th>12</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>07. Targeted Cybersecurity Attacks on Saccos</th>
<th>13</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>08. What should the Exco and Board focus on?</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>How much Visibility do we have on the current controls put in place?</td>
<td>15</td>
</tr>
<tr>
<td>What is our exposure?</td>
<td>15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>09. Maturity Benchmarking - Banks vs Saccos</th>
<th>16</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>10. Cloud - the next frontier for Saccos</th>
<th>18</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>11. Top Priorities for Saccos</th>
<th>19</th>
</tr>
</thead>
</table>
Acknowledgement

This report was prepared by the Serianu CyberThreat Intelligence Team.

We would like to single out individuals who worked tirelessly and put in long hours to deliver this document:

- **Brencil Kaimba** - Editor-in-Chief
- **Barbara Munyendo** - Cyber Intelligence Lead Researcher
- **Nabihah Rishad** - Risk and Top Trends Lead Researcher
- **George Kiio** - Cyber Intelligence Researcher
- **Morris Ndung’u** - Cyber Intelligence Researcher
- **Margaret Ndung’u** - Cyber Intelligence Researcher
- **Enid Mwayuli** - Cyber Intelligence Researcher
- **Salome Njoki** - Survey and Analysis
- **Brilliant Grant** - Survey and Analysis
Introduction

Over 95% of organisations within Africa operate below the Cybersecurity poverty line. This was the take home from the recently published Africa Cyber Security Report 2017. The Cybersecurity Poverty Line means the point below which an organisation cannot effectively protect itself against losses to cyber attacks.

It is with this in mind that we decided to take a deeper look at SMEs, specifically Saccos.

Serianu conducted an extensive survey that incorporated over 100 Sacco representatives across Kenya. The goal was simple: identify the exact pain points facing Saccos and design steps that help address these challenges.

Throughout our analysis and market research, it became undoubtedly clear that Saccos are now a lucrative target for attackers and stand to lose the most with the recent increase in Cyber threats due to limited visibility on their enterprise’s Cyber security posture.

Based on the sheer market size and value of processed transactions within Saccos, our projections indicate that attacks targeting Saccos will double in the next year.

It’s with this in mind that Serianu sought out to provide more insights to help curb the rising threats. Welcome to the 1st Edition of Serianu’s Sacco Cybersecurity Report. We have split this year’s report into various sections to provide the readers with in-depth analysis of:

- What are the top challenges
- How can organisations address these challenges
- What are the top concerns for executives?
- How can these concerns be addressed?
- How can Saccos simplify and meet their compliance needs with SASRA guidelines on Cyber risk management?

The report begins by addressing and analyzing the major changes that have occurred within the Sacco industry and further narrow down to the problematic issues and trends in cyber security and the Sacco industry’s initiatives to solve them.

The next section looks at the results of the Survey analysis which reflect the current state of Saccos. We conducted a survey on over 100 Sacco representatives. This survey aimed to demystify the current practices, most pressing technical security challenges that Sacco’s face. We then grouped and abstracted those challenges. We present an extensive overview of this current state in this section.

The Cyber Intelligence section looks at the top attacks, threats and attack vectors leveraged against Saccos. This was done through our refined methodology of applications, websites and web facing assets review which revealed a number of weaknesses that Saccos need to address. We present an extensive overview of this current state in this section.

Our experience and insights from industry thought leaders enabled us to draft the way forward, priorities and expected legal and compliance issues during the next two to four years. What threats and breaches do we expect to see? Will legislation, and regulatory actions affect this environment? And what responses do we anticipate from cloud service providers and security vendors?

Our final long-lens story is about Maturity curve for Sacco’s. In this section, we provide insightful roadmaps about the specific measures that the current Saccos need to take in order to be competitive in the near future, hereby referred to as the 2030 Sacco.
### Highlights

The past year was a particularly tough period for local organisations with respect to cyber security. The number of threats and data breaches increased with clear evidence that homegrown cyber criminals are becoming more skilled and targeted.

- **Cybersecurity Spending**
  - 97% Spend less than US $10000

- **Cybersecurity Training**
  - 64% Don’t train their employees at all or only do so when an incident occurs

- **Cloud Computing**
  - 40% Are leveraging on Cloud computing capabilities to improve business operations.

- **Cyber Exposure Value**
  - 83% Board members and Exco are now moving away from generic audit reports and are seeing to understand quantifiable metrics on visibility and exposure for the organisation.

- **Skill Shortage**
  - 97% There is a huge Cybersecurity skill shortage within the Saccos particularly for mid and senior level hires.

- **Cybersecurity Management**
  - 83% Manage their Cyber security in-house. This is particularly worrying considering that the skill shortage is highest in Sacco as an industry.
02

Evolution & Impact of Saccos

Saccos have played an important role in uplifting the lives of people in the community through financial inclusion. According to the SASRA Sacco supervision Report 2017, Saccos have a total membership of 3,599,200. Hence Saccos provide services to more than three million Kenyans and frequently offer services which cannot be found elsewhere. For instance, in rural areas many farmers depend on their Saccos for credit and payment services.

Consequently, better financial inclusion has led to increased wealth and employment among Kenyans as well as better physical and mental health, education, recreation and social belonging.

Economic Impact of Saccos in Kenya

The Sacco Supervision Report 2017 by SASRA provides an insightful look into the performance and growth of Saccos over the years as described below.

Gross Domestic Product

According to the Kenya Financial Sector Stability Report 2017, Saccos contributed to 5.72% of Kenya’s GDP controlling Ksh. 442.9 Billion. Furthermore, Saccos have a total of 3,599,200 members.

Revenue Growth

The report indicated that the total asset base of deposit taking Saccos has been on a steady increase in the past three years.

In 2017, the total assets portfolio of deposit taking Saccos grew to reach Kshs. 442.3 Billion from Kshs. 393.5 Billion in 2016 reflecting a 12.4% growth rate. In 2015, the total asset base had been recorded to be Ksh. 342.8 Billion.
Number of Employees

The number of employees working for Saccos increased in the year 2016 to 8,194 employees from 6,245 employees in 2015. This further goes to prove that Saccos are indeed improving the quality of lives of households in Kenya.

Evolution of Co-operative Societies in Kenya

- **1908**: Formation of Lumbwa Cooperative
- **1931**: Kenya Cooperative Creameries (KCC) formed
- **1937**: Kenya Planters Cooperative Union (KPCU) formed
- **1950-1952**: 160 cooperatives formed during this period
- **1958**: More than 400 cooperatives registered
- **1999**: The number of registered cooperatives had risen to 7,000
- **2003**: Registered cooperatives reach 10,297
- **2009**: Sacco Societies Regulatory Authority (SASRA) formed
- **2012**: First diaspora Sacco, the Kenya USA Diaspora Sacco was registered
State of Cyber Security in Saccos

This section provides an analysis of findings from the Survey conducted during the 2018 SASRA workshop for board and CEOs held in June 2018 in Mombasa, Kenya. 125 deposit taking Saccos representatives participated in this survey. We asked the respondents, who included Chief Executive Officers, IT Directors, IT Managers and Board Chairs, questions regarding the state of Cybersecurity within their respective Saccos. Below are the detailed findings.

Cybersecurity Budget

Approximately how much does your organisation spend annually on cybersecurity?

Allocated between $1-10000 for cyber security

- 56% spend $1-10000
- 15% spend $0
- 10% spend $1001-5000
- 6% spend $5000-10000
- 3% spend $10000+
- 10% don’t know

This shows that most Saccos do not invest heavily on cybersecurity which means less security measures are put in place to guard against potential attacks.

Cybersecurity Training

How often is your staff trained on cybersecurity risks?

- 50% of Saccos do not have an established Cybersecurity training program on cyber risks
- 40% of staff trained only if there is a problem
- 24% of staff never trained
- 10% of staff trained monthly
- 1% of staff trained weekly

The Saccos that never conduct awareness essentially exposes the Saccos to attacks that can be facilitated through social engineering.

BYOD Usage

Does your SACCO allow BYOD usage and do you have a BYOD Policy in place?

- 38% of Saccos allow the use of Bring Your Own Devices while
- 66% of these Saccos have a best practice policy for BYOD
- 24% of staff never trained
- 1% of staff trained weekly

BYOD usage increases the number of attack vectors that an attacker would use to gain unauthorized access into a SACC. Hence, it is crucial that all Saccos permitting BYOD usage should have a working BYOD policy in an effort to mitigate the potential threats.

Cloud and IoT

Does your SACCO allow Cloud and IoT usage and do you have a Cloud and IoT Policy in place?

- 40% of Saccos have adopted Cloud and IoT Technologies while
- 23% have a Cloud and IoT policy

Demystifying Cybersecurity for Saccos
This shows that there is a gap when it comes to mitigating cyber security risks that may arise from the usage of Cloud and IoT technologies.

**Cybersecurity Management**

How does your SACCO handle cybersecurity management?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Management Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>83%</td>
<td>Manage inhouse</td>
</tr>
<tr>
<td>7%</td>
<td>Outsourced to an ISP</td>
</tr>
<tr>
<td>6%</td>
<td>Outsourced to a MMSP</td>
</tr>
</tbody>
</table>

A critical trait however, noted with in house managed Cyber security is that, usually the system Administrators double up as the personnel in charge of security. As a result, majority of these setups lack sufficient skillsets, time and resources to fully manage this role.

**Skill Gap**

Is your SACCO equipped with all the necessary skills?

Skill shortage observed in the Saccos cut across various levels in the organisational structure of the Saccos.

<table>
<thead>
<tr>
<th>Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Management</td>
<td>31%</td>
</tr>
<tr>
<td>Mid Management</td>
<td>29%</td>
</tr>
<tr>
<td>Mid Junior</td>
<td>20%</td>
</tr>
</tbody>
</table>

The 2017 Ransomware attack brought to light the real implications of limited skill particularly within Saccos. During the attack, Cybersecurity professionals in Africa were contracted by established organisations. At the height of the crisis, the small cyber security professional’s talent pool were snapped up by huge multi-nationals that offered better incentives. This left the Saccos completely at the Cyber criminals mercy.

**Further analysis on skill gap revealed the following:**

- Demand for cybersecurity professionals is strongest in banking sector, followed by Insurance and then Saccos.
- Severe cyber security skills shortages persist in every industry with Saccos and Insurance being the worst affected.

**How can Saccos tackle this Skill gap?**

- Growing talent in-house - Technical Training is key to ensure that we equip the IT teams with the right skills to Anticipate, Detect, Respond and Contain cyber threats.
- The skills shortage can only be rectified if the Saccos commit to building talent from the junior level to the senior management level.
Threats Due to Digitization and Mobile Usage

The following mobile application vulnerabilities were identified:

- **Sensitive Data Protection Vulnerability**
  - Allows users to retrieve sensitive information such as usernames and passwords.

- **Improper SSL Validation/SSL Pinning**
  - Allows attackers to perform man-in-the-middle attacks between the Sacco and its customers.

- **Cryptographic Vulnerabilities**
  - Allows malicious attackers to intercept customer’s transaction details such as credentials, account details and PIN.

- **Reverse Engineering Vulnerability**
  - Allows attackers to change the normal operations of the mobile apps resulting in attackers posting fake applications online.

- **Use of Dangerous API**
  - Implements methods which allows JavaScript to control the host application.
Server Vulnerabilities

The following server vulnerabilities were identified:

**Cryptographic Vulnerabilities**
Use of a self-signed certificate that is not associated to a trusted Certificate Authority (CA).

**Path Vulnerabilities**
Disclosure of web directories, backup files and application code allowing an attacker to retrieve information.

**Deprecated Software**
Mobile application running on a deprecated versions of Apache and PHP.

**Clickjacking**
Hosting of a web application that is vulnerable to clickjacking.

**Availability Vulnerability**
Mobile application server running a DNS Service that is vulnerable to DDoS.

**Sensitive Data Protection Vulnerability**
Hosting of a web application that has some Methods enabled that can be used to debug web server connections.

**Authorization Vulnerability**
Mobile application server running an SMB service that does not require SMB signing. SMB Signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB.

**Authentication Vulnerability**
Mobile application server hosting critical services without restrictions other than authentication.
Sacco Industry Challenges

Notable challenges facing the SACCO industry over the past year include:

Digital Transformation
In order to stay competitive and improve customer engagement, Saccos are adapting newer forms of technology. However, most of these Saccos lack a clear digital strategy and vision for the organization as well as a well-defined road map for digitization. In addition, security is still a challenge that needs to be addressed when adopting digital platforms.

Automation of Processes
Saccos have been at the forefront of technology and automating their manual processes as much as possible. There exists a gap in fully understanding the internal business processes that are being automated as well as the related technology and security requirements. This has also led to the exposure to various types of threats which may lead to damages and significant financial loss.

Mobility
Many Saccos are now offering their customers more convenient ways of accessing services. There has been a rise in mobile and web applications within the SACCO industry. Attackers are now leveraging these platforms to perpetrate attacks such as malware attacks and compromising poor application designs and configurations.

Cloud and Outsourcing
The cloud has presented an opportunity for the SACCO industry to increase their agility and transform their business operations. With the increased storage of sensitive data on the cloud, attackers are now able to access this data and use it to compromise the organization. Data breaches result in diminished trust by customers which results in loss of business.

Growth in Members
Over the past few years, the SACCO industry has grown significantly. Saccos make a significant contribution to economic growth within the country. Most organizations have not yet developed strategic plans to anticipate and prepare for cyberattacks that are as a result of this growth. Executives need to plan ahead as these attacks can cost Saccos money, customers, productivity, investments, opportunities, and growth.
Targeted Cybersecurity Attacks on Saccos

As a result of these trends, there has been an increase in cyber-attacks specifically targeting the SACCO industry. Over the past year, the top six targeted attacks on Saccos are as below:

**Database Breaches**
Saccos are now becoming an easy target for attackers leveraging database manipulation attacks. The goals of data manipulation attackers are as diverse as the Saccos they target. The most popular goal seen in this industry is where the attackers exploit this attack to make a profit. After informing the victims that their systems have been compromised, the attackers refuse to change back the data until a ransom has been paid to them.

**Abuse of Privileged Access**
Privileged account abuse occurs when the privileges associated with a particular user account are used inappropriately or fraudulently, either maliciously, accidentally or through willful ignorance of policies. This attack has led to the loss of sensitive data and business intelligence within Saccos as well as downtime of systems and applications essential for business operations.

**Malware (Keyloggers)**
Keyloggers are usually employed in conjunction with other malicious programs, capturing keystrokes and sensitive information such as customers’ account numbers, passwords, and other sensitive information. Attackers are leverage this attack to steal corporate confidential data, impersonate users or carry out fraudulent financial transactions within Saccos.

**Critical Data Manipulation**
Critical data describes the core entities of the enterprise including customers, prospects, suppliers, branches, account details. Due to the lack of a clear process of cleaning, governance, tracking and control of all master data within Saccos, attackers have been able to compromise information systems and steal sensitive data.

**Email Phishing Attacks**
Phishing attacks have been on the rise within the SACCO industry. As Saccos succumb to such attacks, the effects include financial losses, declining market share, reputation, and consumer trust. Depending on the depth of the attack Saccos may have a more difficult time recovering.

**Ransomware**
For Saccos, ransomware can be devastating to productivity as it puts all projects on hold until access to important files is regained and the system is secured. All sensitive information is at risk of falling into the wrong hands and being erased from devices. A data breach leads to sensitive customer and organizational information being at risk.
What Should the Exco and Board Focus on?

Top Cybersecurity Concerns for CFOs, CEOs & Board Members

1. Why am I investing in security infrastructure and what’s the ROI?
2. How do I know that we’ve actually lowered our Cyber risk exposure?
3. As my business undergoes digital transformation, how can I get the quickest view of the impact on my overall corporate risk?

Top Concerns for CIO, CISO and CRO

1. Is the investment provided thus far going to the more critical areas of risk, and is it having the desired effect?
2. How do we get a clear approach to answer the deceptively difficult question “How secure are we?”
3. My organisation has a fragmented view of its security posture. How do I gain control and full visibility?
4. How can we effectively communicate our progress to the board, regulators and other stakeholders?
To fully address these concerns, the Exco and Board need to adopt a unified risk quantification approach that will enable them to measure and quantify their cyber security risk. This requires coordination within the entire enterprise Business and IT. Board members should therefore seek to answer the following questions.

**Q1. How much Visibility do we have on the current controls put in place?**

**Controls - Measure Control Environment Maturity Score**

It is critical to establish the current state of an organisation’s business processes, performance metrics and set a roadmap of key milestones needed in order to optimize the cybersecurity posture. Cybersecurity Maturity is a great way to determine whether an institution’s behaviors, practices, and processes can support cybersecurity preparedness within the following four domains:

- **Anticipate Risk**
  - Cyber Risk Management
- **Detect Vulnerabilities**
  - Cyber Vulnerability Management
- **Respond to Incidents**
  - Cyber Incident Management
- **Contain Threats**
  - Cyber Threat Management

**Q2. What is our exposure?**

**Exposure - Determine Breach Scenarios and Exposure Value**

It is critical that as an organisation you develop different breach scenarios based on the profile of an organisation’s risk profile, services, business applications, computing environment, and their defensive posture. The organisations should simulate specific cyber incidents and breaches to estimate possible exposure relative to implemented controls.

Using local, global and breach-specific historical loss data estimates the financial consequences of the potential loss for each exposure is then estimated. This enables an organisation to identify exposure and deficiencies to evaluate how risk can be reduced through a combination of risk mitigation and risk transfer.
Maturity Benchmarking - Banks vs Saccos

Direct comparison may seem unfair at first, but Banks and Saccos both shared promising beginnings, similar threat landscapes. Despite this, we are seeing more difficulty trying to convince the Saccos and other SME alike about the value of investing in Cybersecurity controls.

Using the Africa Cyber Security Maturity Framework, we establish the maturity levels of organisations.

- **Ignorant**: Falling well short of baseline security practices and thus neglecting its responsibility to properly protect its IT assets. Many enterprises lack a holistic understanding of their cyber risks and therefore, an effective strategy to address these risks.
- **Informed**: Has generally implemented some security best practices and thus making progress in providing sufficient protection for its IT assets.
- **Engaged**: Has a well-developed security program and is well positioned to further improve its effectiveness.
- **Intelligent**: Has a superior security program and is extremely well positioned to defend its IT assets against advanced threats.
- **Excellent**: A comprehensive IT security program is an integral part of the culture. Status metrics for the IT security program are established and met.
Below is an analysis of Sacco’s vs Banks in general

Majority of Saccos
- Basic Network Protection
- Ad Hoc Infrastructure & Application Protection
- IT Service Desk & Whistleblowing
- Traditional Signature-Based Security Controls
- Ignorant

Majority of tier 2 Banks
- Acceptable Usage Policy
- General Information Security Training & Awareness
- IT BC & DR Exercises
- IT Cyber Attack Simulations
- Informed

Operational Excellence
- Situational Awareness of Cyber Threats
- Basic Online Brand Monitoring
- Online Brand & Social Media Policing
- Ad-hoc Threat Intelligence Sharing with Peers
- Government/Sector Threat Intelligence Collaboration
- Excellent

IT Cyber Attack
- Enterprise-Wide Infrastructure & Application Protection
- 24x7 Technology Centric Security Event Reporting
- Identity-Aware Information Protection
- Adaptive & Automated Security Control Updates

Business-Wide Cyber Attack Exercises
- Targeted Intelligence-Based Cyber Security Awareness
- Business Partner Cyber Security Awareness

Sector-Wide & Supply Chain Cyber Attack Exercises
- Cross-Channel Malicious Activity Detection
- Tailored & Integrated Business Process Monitoring

Security Event Monitoring
- External & Internal Threat Intelligence Correlation

Network & System Centric Activity Profiling
- Workforce/Customer Behaviour Profiling

Operational Excellence
- Real-time Business Risk Analytics & Decision Support

Adaptation & Automated Security Control Updates
- External Threat Intelligence

Ad-hoc Threat Intelligence Sharing with Peers
- Criminal/Hacker Surveillance

Targeted Cross-Platform User Activity Monitoring
- Baiting & Counter-Threat Intelligence

Cross-Channel Malicious Activity Detection
- Internal Threat Intelligence

External Threat Intelligence
- Intelligence Collaboration

Business Partner Cyber Security Awareness
- Business Process Monitoring

Training & Awareness
- Cyber Attack Preparation

Behavioural Analytics
- Targeted Intelligence-Based Cyber Security Awareness

Government/Sector Threat Intelligence Collaboration
- Targeted Cross-Platform User Activity Monitoring

Internal Threat Intelligence
- Cyber Attack Preparation

E-Discovery & Forensics
- Automated Electronic Discovery & Forensics

IT Cyber Attack
- Ad-Hoc System/Malware Forensics
- Ad-hoc Threat Intelligence Sharing with Peers

Real-time Business Risk Analytics & Decision Support
- Criminal/Hacker Surveillance

IT BC & DR Exercises
- IT BC & DR Exercises

IT Service Desk & Whistleblowing
- Security Log Collection & Ad Hoc Reporting

Social Media Policing
- Ad Hoc Infrastructure & Application Protection

Ignorant
- Basic Network Protection

Informed
- Acceptable Usage Policy

Engaged
- General Information Security Training & Awareness

Intelligent
- IT Cyber Attack Simulations

Excellent
- Business-Wide Cyber Attack Exercises

Cyber Security Maturity Levels
- Ignorant
- Informed
- Engaged
- Intelligent
- Excellent

Proactive Threat Management
- Blissful Ignorance

Transformation
- Transformation
Cloud - the Next Frontier for Saccos

Looking back at immeasurable impact of Saccos on the Kenya people and economy – from crowdfunding, employment creation and loan services – chances are, we yet to fully exploit these benefits to the maximum.

At the same time, however, it’s important to note that majority of the Saccos are not positioned to take advantage of these opportunities. It’s therefore important to map where we are today with the technology, and, how we can take advantage of the technological advancements to reduce costs and ensure continued security of critical infrastructure and assets.

Cloud computing is arguably the most crucial development for Saccos.

Current Operating Models for Cloud

<table>
<thead>
<tr>
<th>Cloud Service Offered</th>
<th>What It Is</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td>IaaS is the lowest level of cloud solution and refers to cloud-based computing infrastructure as a fully-outsourced service. An IaaS provider will deliver pre-installed and configured hardware or software through a virtualized interface. Examples of IaaS offerings are managed hosting and development environments.</td>
</tr>
<tr>
<td>Platform as a Service (PaaS)</td>
<td>This type of cloud computing is similar to IaaS but is more advanced. With PaaS, apart from simply providing infrastructure, providers also offer a computing platform and solution stack as a service.</td>
</tr>
<tr>
<td>Platform as a Service (PaaS)</td>
<td>This type of cloud computing is similar to IaaS but is more advanced. With PaaS, apart from simply providing infrastructure, providers also offer a computing platform and solution stack as a service.</td>
</tr>
<tr>
<td>Software as a Service (SaaS)</td>
<td>SaaS providers provide fully functionally web-based applications on demand to customers. The applications are mainly targeted at business users and can include web conferencing, ERP, CRM, email, time management and project tracking among others.</td>
</tr>
<tr>
<td>Recovery as a Service (RaaS)</td>
<td>Recovery as a Service (RaaS) solutions helps companies to replace their backup, archiving, disaster recovery and business continuity solutions with a single, integrated platform. RaaS providers protect and can help companies recover entire data centers, servers (OS, applications, configuration and data) and data (files and databases).</td>
</tr>
</tbody>
</table>
Top Priorities for Saccos

To help Saccos meet their cybersecurity requirements, Serianu has developed a checklist for Managed Security Services based on industry regulations and Cybersecurity best practice standards. It provides direction on what Saccos need to properly assess risk, monitor and detect threats on their network, develop plans for incident response, and create customized reporting for compliance and regulatory purposes.

1. **Awareness and Training**
   Right from the board members, Senior management, Technical and non-technical teams. Its critical that users are empowered with the right skills to identify and proactively respond and contain threats. With attackers now performing targeted attacks on specific members, it’s also crucial that Saccos develop and implement security awareness training programs. This can be done in-house or outsourced. Regardless of the mode of training, an organisation should ensure that a needs assessment is conducted before adopting any form of employee training program.

2. **Continuous Monitoring and Log Analysis**
   As indicated in the report, Saccos are now as much a lucrative target as banks. Its paramount that Saccos monitor their environments.

3. **Visibility and Exposure Analysis**
   In this era where the threat landscape is evolving and threat vectors (BYOD, IoTs) increasing daily, there is need for maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Its critical for Saccos to conduct inherent risk profiling, maturity assessment to determine their visibility and exposure.

4. **Continuous Risk Assessment and Treatment**
   SASRA released a Risk guidance framework that provides guidelines on the frequency of risk assessment. With the numerous attacks occurring as a result of missing patches and susceptibility to malware, it’s critical for Saccos to focus on developing vulnerability and patch management programs within their institutions. This will involve running periodic and automated vulnerability scanners on the network which can identify vulnerabilities such as buffer overflow, open ports, SQL injections, obsolete systems and missing patches. Use of antivirus software is also crucial for detecting and removing malware. All in all, the most important part is correcting the identified vulnerabilities which will involve the installation of a patch, a change in network security policy, reconfiguration of software (such as a firewall) and/or educating users about social engineering.

5. **Managed Services and Independent Reviews**
   With the increase in work overload of in-house security teams, higher pressure to show ROI quickly and higher potential for collusion between security analyst and an inside attacker, there is need for Saccos to look at the option of engaging the services of managed service providers. These providers come with a wide range of expertise to manage security related incidents and provide independent reviews for the organisation.
Compliance: SASRA Guidelines on Cyber Security Risk Management

The Sacco Societies Regulatory Authority herein referred to as (SASRA) has released a set of guidelines on Cyber Security Risk Management for Deposit-Taking Saccos. These guidelines set the minimum standards that DTS should adopt to develop effective Cybersecurity governance and risk management frameworks.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
<th>Serianu’s Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Governance: This refer to measures put in place to manage Cyber security risks.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Role of Board** | Board of Directors have the ultimate responsibility over Cybersecurity. | **Oversight from the Top:** Boards need to have an understanding of Cyber risks and threats within Saccos. This means:  
- Cybersecurity awareness for the board  
- Defining clear metrics for measuring and monitoring the performance and effectiveness of Cybersecurity program. |
| **Role of Senior Management** | Senior managers are responsible for the implementation and monitoring of Cybersecurity policies, controls and procedures. | **Determine and Reduce the Cyber Risk Exposure Value:** Senior managers should focus on determining their Cyber Risk Exposure and implement controls to minimize this exposure. Focus should be on understanding the business environment in terms of:  
- **People Skills:** Empower the people with the required technical and analytical skills to Detect, Respond and Contain Cyber threats.  
- **Process:** Defining operation procedures for all business critical processes as per best practice.  
- **Technology:** Put in place the right technology to support Cybersecurity. |
| **Risk Assessment** | Identify and analyze cyber risks facing the organisation. **Deliverables:** A comprehensive report shared with Senior management, Board and Authorities within 30 days. | **Inherent Risk Profiling:** There are a number of risks that organizations automatically adopt by virtue of the industry they operate in. For example  
- Regardless of size or location, a Sacco will face credit risks, interest rate risks, market risk, and operating and liquidity risks.  
- When a Sacco, regardless of industry, opens up a Mobile channel to their environment, there is an inherent risk that automatically arises.  
As such, it is important to understand the environment you are operating in, as this forms your inherent risk. |
| **Information Security Incidence Report to the Authority** | All Cyber security related incidences that are likely to disrupt the operations of the Sacco for more than 12 hours and/or make the Sacco suffer financial loss of more than Ksh. 200,000 should be reported to SASRA. | **Security is never 100% full-proof,** hence, its critical to have contingencies in place. This includes An incident response team, Escalation matrix and Backups. |
| **Asset Management** | Implement processes and tools used to track, control, prevent and correct secure access to the Sacco’s assets. | **Know thy self.** Without fully knowing what assets an organisation has, it’s virtually impossible to protect and defend it against cyber criminals  
Asset management will forms the foundation for a successful  
- Vulnerability and patch management program  
- Monitoring program |
<table>
<thead>
<tr>
<th>Protection Access Controls</th>
<th>There are a number of risks faced by Saccos if access control measures are not put in place. Consider the cases below:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Attackers can escalate their privileges on victim machines by launching password guessing, password cracking, or privilege escalation exploits to gain administrator control of systems, which they can then use to propagate to other machines across a Sacco’s environment.</td>
</tr>
<tr>
<td></td>
<td>2. Attackers can compromise an inactive user’s account left behind by temporary workers, contractors and former employees. This also includes accounts left behind by the attackers themselves.</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>The default configurations for network infrastructure devices are geared for ease-of-deployment and ease-of-use rather than security. Open services and ports, default accounts or passwords, support for older protocols as well as pre-installation of unneeded software can all be exploitable in their default state.</td>
</tr>
<tr>
<td></td>
<td>Attackers search for vulnerable default settings, electronic holes in firewalls, routers, and switches and use these to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker can gain access to sensitive data, alter important information or even use a compromised machine to pose as another trusted system on the Sacco’s network.</td>
</tr>
<tr>
<td>Vulnerability &amp; Patch Management</td>
<td>Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. This is because:</td>
</tr>
<tr>
<td></td>
<td>1. Attackers continually scan for vulnerable software and exploit it to gain control of a target’s machines.</td>
</tr>
<tr>
<td></td>
<td>2. Attackers can easily exploit new vulnerabilities on systems that lack critical patches</td>
</tr>
<tr>
<td></td>
<td>A patch management program should be put in place to ensure that software and firmware patches are applied in a timely manner.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records, they are blind to the details of the attack. Without solid audit logs, an attack may go unnoticed indefinitely. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs so they do not know that their systems have been compromised.</td>
</tr>
<tr>
<td>Incident Response and Recovery</td>
<td>Cyber incidents are now just part of our way of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyber-attack against an enterprise is not “if” but “when”.</td>
</tr>
<tr>
<td></td>
<td>Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker’s presence and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly infiltrate more sensitive data than would otherwise be possible if an effective incident response plan were in place.</td>
</tr>
</tbody>
</table>
# Incident Response
Implement processes and tools used to manage, recover, and contain their environment after an attack has occurred.

Cyber incidents are now just part of our way of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyber-attack against an enterprise is not “if” but “when”. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker’s presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly infiltrate more sensitive data than would otherwise be possible were an effective incident response plan in place.

# Security Awareness
Implement processes to train employees on various cyber defense approaches and good cyber defense habits.

It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. Examples include:

- End users can fall prey to social engineering schemes such as phishing
- IT operations may not recognize the security implications of IT artifacts and logs
- Security analysts may struggle to keep up with an explosion of new information
- System developers and programmers may not understand the opportunity to resolve root cause vulnerabilities early in the system life-cycle
- Executives and system owners may struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions

Empowering people with good cyber defense habits can significantly increase readiness.

# KYC - Know Your Customers
Saccos are required to conduct due diligence on their customers.

KYC is critical particularly for Transactions Monitoring. Saccos need to embrace a dynamic approach into transaction monitoring that focuses on the following:

- **Threshold Analysis**
  - Volume
  - Velocity
  - Limits
  - Multiplicity
- **Profile Analysis**
- **Correlation**

**Multiplicity**: This refers to an anomaly in the way an asset or a user interacts with its environment. Example Transactions from Dormant accounts.

**Velocity**: In this context, it refers to the frequency of occurrence of an action or an event. Example Unusual multiple transactions or balance requests within a short period of time

**Volume**: As used in this document refers to the number of events received over a period of time. Example, unusually large withdrawals within a short period.

Dynamic analysis allows an organisation to determine malicious activities within the network and trend patterns.
For more information, contact:

Serianu Limited,
14 Chalbi Drive, Lavington
P. O. Box 56966 - 00200,
Nairobi, Kenya

General Information: +254 (0) 20 200 6600
Cyber Crime Hotline: +254 (0) 800 22 1377
Email: info@serianu.com
http://www.serianu.com