Cybersecurity & Data Protection in the Middle East

Cybersecurity Strategic Approach, SAMA CSF Overview & Best Practices, Tips to Prevent Potential Cyber Attacks

databrackets

info@databrackets.com

866-276-8309

databrackets
cybersecurity • audit • compliance

Disclaimer

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

Ultimately attorneys have the last word.

Agenda

- Cybersecurity Strategic Approach
- SAMA Cyber Security Framework (CSF) Overview & Best Practices Implementation
- databrackets' Cybersecurity Compliance platform for SAMA
- Tips to prevent potential cyber-attacks

About Us

DIY TOOLKIT

DIY assessment, training, customized policies & procedures and much more …

CONSULTING

Professional services to help you with your Compliance needs

MANAGED SERVICES

Managed compliance and security services to focus on your key business outcome.

Cybersecurity and Privacy Audit | Compliance | Certification & Attestation| databrackets

- HIPAA/HITECH
- PCI Data Security
- CCPA
- OSHA
- GDPR
- Penetration Testing
- FDA CFR Part 11
- ISO 27000 Series
- Cloud Security Assessment
- NIST Framework
- Cybersecurity Framework
- SOC Certification
- Third Party Risk Assessment
- NYDFS Cybersecurity
- Custom Assessment

The slide lists majority of our programs and services mainly in Cybersecurity and Privacy Audit, Compliance, Certifications & Attestation Areas.

Logistics

- How do I ask questions?
- Can I get a copy of the presentation deck?
- Will a recording be available?
- How can I contact you later?
- How can I get more information about anything that is presented today?

All webinars are recorded and available as an “on demand” subscription.

Speaker

Srini Kolathur

CISSP, CISA, CISM, MBA

Director, databrackets

Srini's Background

- Security and Compliance
- Cisco IT Infrastructure
- HIPAA, PCI, Sarbanes-Oxley and ISO 27k Series
- A member of Rotary Club of Morrisville
- Interests: Running, healthy living and giving back

Guest Speaker

Ravi Prakash

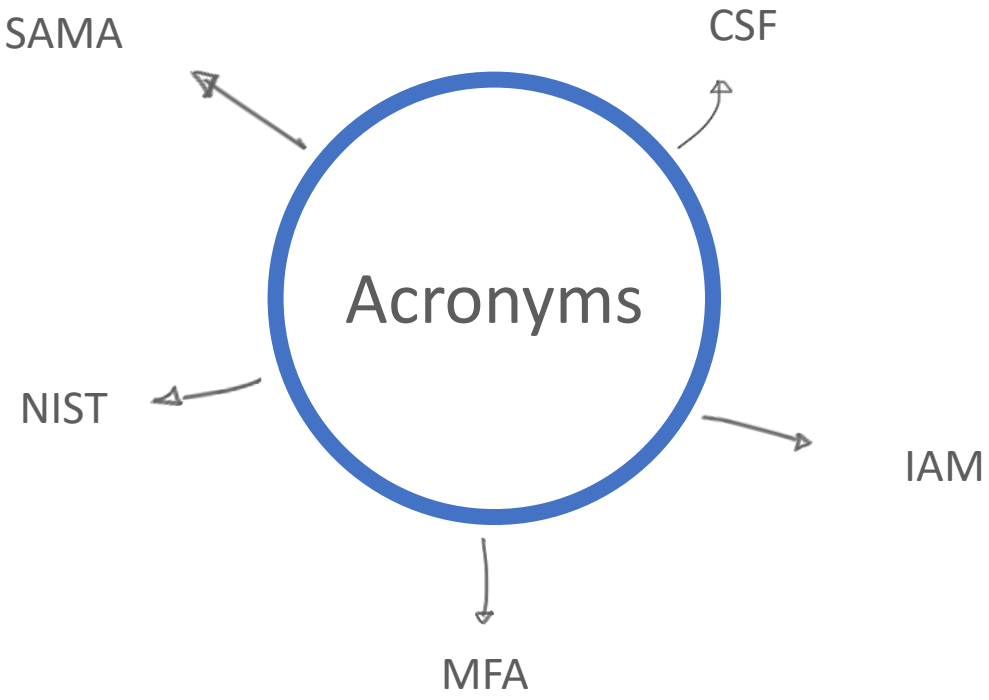
CISM, CDPSE, GRCP, GRCA, ISO 27001 LA, ISO 22301 LA, ISO 20000 LA, ISO 27701 LA, ISO 9001 LA

Sr. Consultant, Paramount Computer Systems, KSA

Ravi's Background

- Cybersecurity GRC
- Information Security Management System implementation (SAMA CSF, CITC, NCA Requirements, NIST, ISO 27001:2013)
- IT Audits, General Controls Review
- Cloud Security
- Third party risk management

Terms You May Hear



Everyone and everything has an acronym.

Why Should You Care?

- ✓ **Data Breach incidents**
  - Identity theft
  - Malware including ransomware
  - Cyber attacks and other frauds
- ✓ **Violation of Data Protection Rules**
  - Penalties
  - Civil
  - Criminal
- ✓ **Loss of Trust**

Top Cybersecurity Statistics you Need to Know

Cyber attacks per day

2,200 attacks each day which breaks down to nearly 1 cyberattack

every 39 seconds!!

Global cyber crime damage by 2021

$16.4 billion per day

$684.9 million per hour

$11 million per minute

$190,000 per second

Did you know?

25% of buyers tend to abandon products and services in favour of competitors upon knowing of a cyberattack

Source: Cybersecurity Ventures, 2020

Data Breach Incidents

- In 2012, ARAMCO Attack in KSA through a computer virus named Shamoon
- In December 2018, a variant of Shamoon malware attacked the Italian offshore contractor SAIPEM's servers in KSA
- In October 2020, hackers exploited a serious Windows vulnerability to target Middle Eastern network technology providers and organizations involved in work with refugees
- In October 2020, a cyber mercenary group targeted government officials and private organizations in the Middle East using a combination of methods including zero-day exploits

Source:researchgate , Arabnews

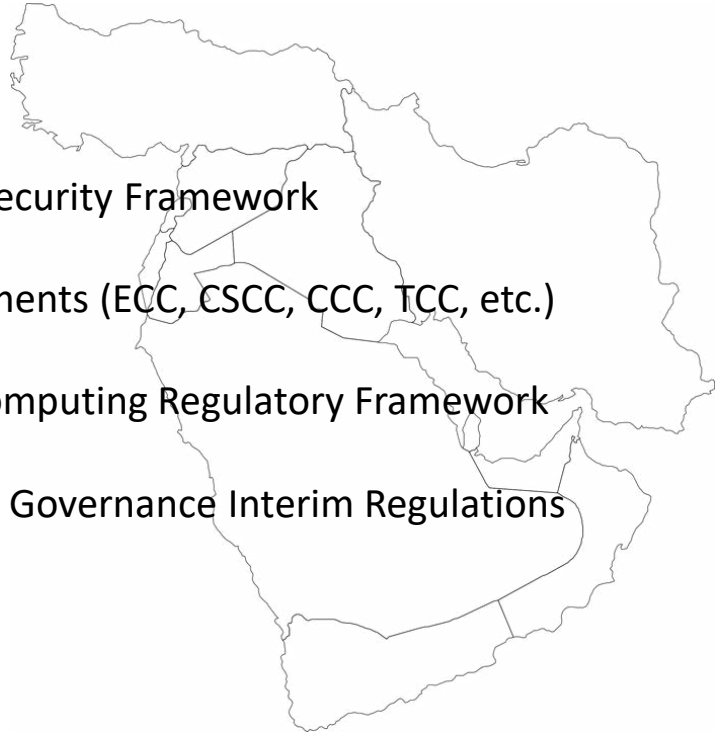
Data Breach Incidents (contd.)

2020 - 2021

84% of Saudi Arabian cybersecurity professionals said attacks increased due to employees working remotely.

Data breaches in the MENA region reached $6.53 million, well above the global average incident cost of $3.86 million, according to a 2020 study by the Ponemon Institute and IBM Security.

Data Privacy and Security Regulations - KSA



Saudi Arabia

1. SAMA Cybersecurity Framework
2. NCA Requirements (ECC, CSCC, CCC, TCC, etc.)
3. CITC Cloud Computing Regulatory Framework
4. National Data Governance Interim Regulations

Data Privacy and Security Regulations - UAE

United Arab Emirates (UAE)

NESA, The National Electronic Security Authority, is a government body tasked with protecting the UAE's critical information infrastructure and improving national cyber security.

NESA Compliance is **mandated to all government organizations, semi-government organizations and business organizations** that are identified as critical infrastructure to UAE.

Other regulations in UAE

Federal Law by Decree No. 3 of 2003 Regarding the Organisation of the Telecommunication Sector, Federal Law by Decree No. 5 of 2012 on Combating Cybercrimes (13 August 2012), Federal Law No. 18 of 1993: Commercial Transactions Law, and the UAE Federal Law No. 2 of 2019

Data Privacy and Security Regulations - Bahrain

1. The Central Bank of Bahrain and Financial Institutions Law 2006, which regulates data protection in the regulated financial activities sector;
2. the Telecommunications Law 2002, which regulates data protection in the telecommunication sector; and
3. PDPL

Data Privacy and Security Regulations – Kuwait and Qatar

Kuwait

1. Data Privacy Protection Regulation, No.42 of 2021
2. Cyber Security Framework for the Kuwaiti Banking Sector

Qatar

1. Law No. 13 of 2016 Concerning Privacy and Protection of Personal Data

Other Standards/Certifications

{databrackets}

SOC 2 Audit certification

SOC 2 audit certification for service organization reports are designed to help service organizations that provide services to other entities, build trust and confidence in the service performed and controls related to the services through a report by an independent CPA.

ISO/ ICE 27001

The ISO/IEC 27000 family of standards helps organizations keep information assets secure.

Introduction to SAMA Cyber Security Framework

SAMA established a Cyber Security Framework (“the Framework”) to enable Financial Institutions regulated by SAMA (“the Member Organizations”) to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services, the Member Organizations must adopt the Framework.

The Framework will be used to periodically assess the maturity level and evaluate the effectiveness of the cyber security controls at Member Organizations, and to compare these with other Member Organizations.

The Framework is based on the SAMA requirements and industry cyber security standards, such as NIST, ISF, ISO, BASEL and PCI.

In 2017, the Saudi Arabian Monetary Authority created the Cyber Security Framework to assist companies in successfully detecting and mitigatingCyber Security threats.

SAMA CSF Applicability & Objective

Applicability of the Framework:

The Framework is applicable to all Member Organizations regulated by SAMA, including:

- All Banks operating in Saudi Arabia;
- All Insurance and/or Reinsurance Companies operating in Saudi Arabia;
- All Financing Companies operating in Saudi Arabia;
- All Credit Bureaus operating In Saudi Arabia;
- The Financial Market Infrastructure

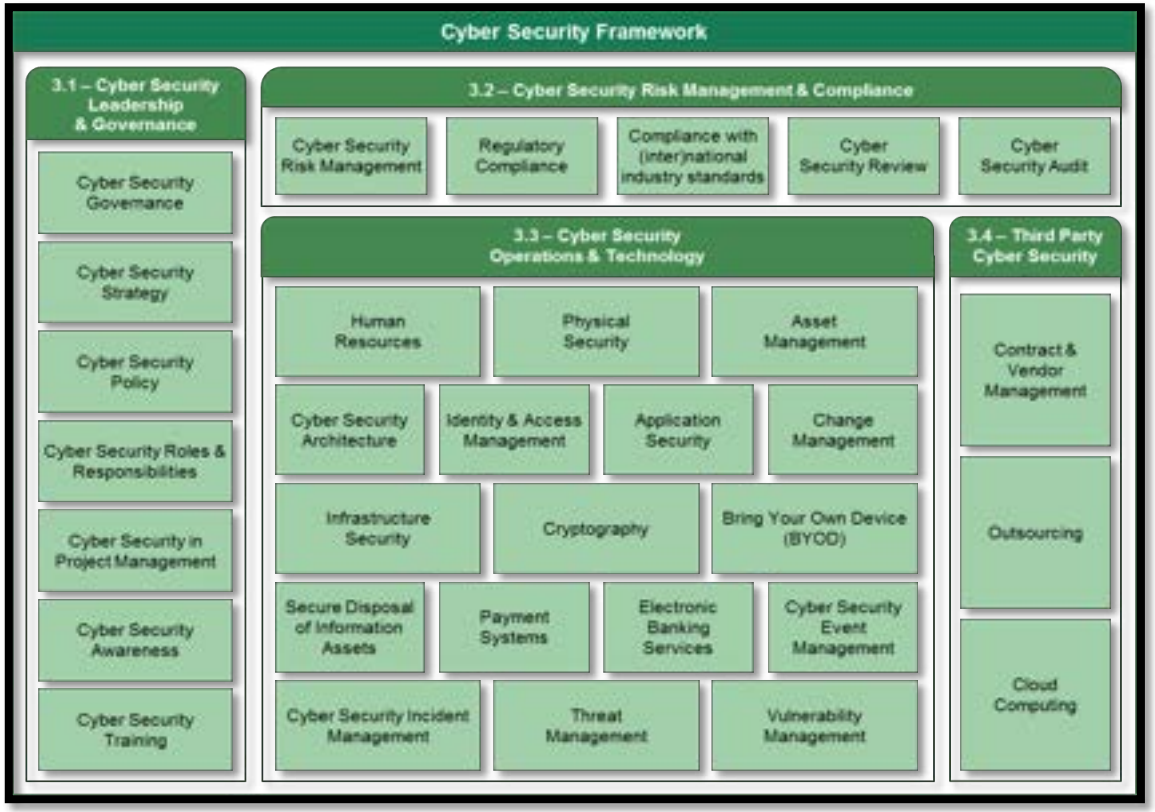
The objective of the Framework

- To create a common approach for addressing cyber security within the Member Organizations.
- To achieve an appropriate maturity level of cyber security controls within the Member Organizations.
- To ensure cyber security risks are properly managed throughout the Member Organizations

SAMA Cyber Security Framework

SAMA CSF The Framework is structured around four main domains, namely:

- Cyber Security Leadership and Governance
- Cyber Security Risk Management and Compliance
- Cyber Security Operations and Technology
- Third Party Cyber Security



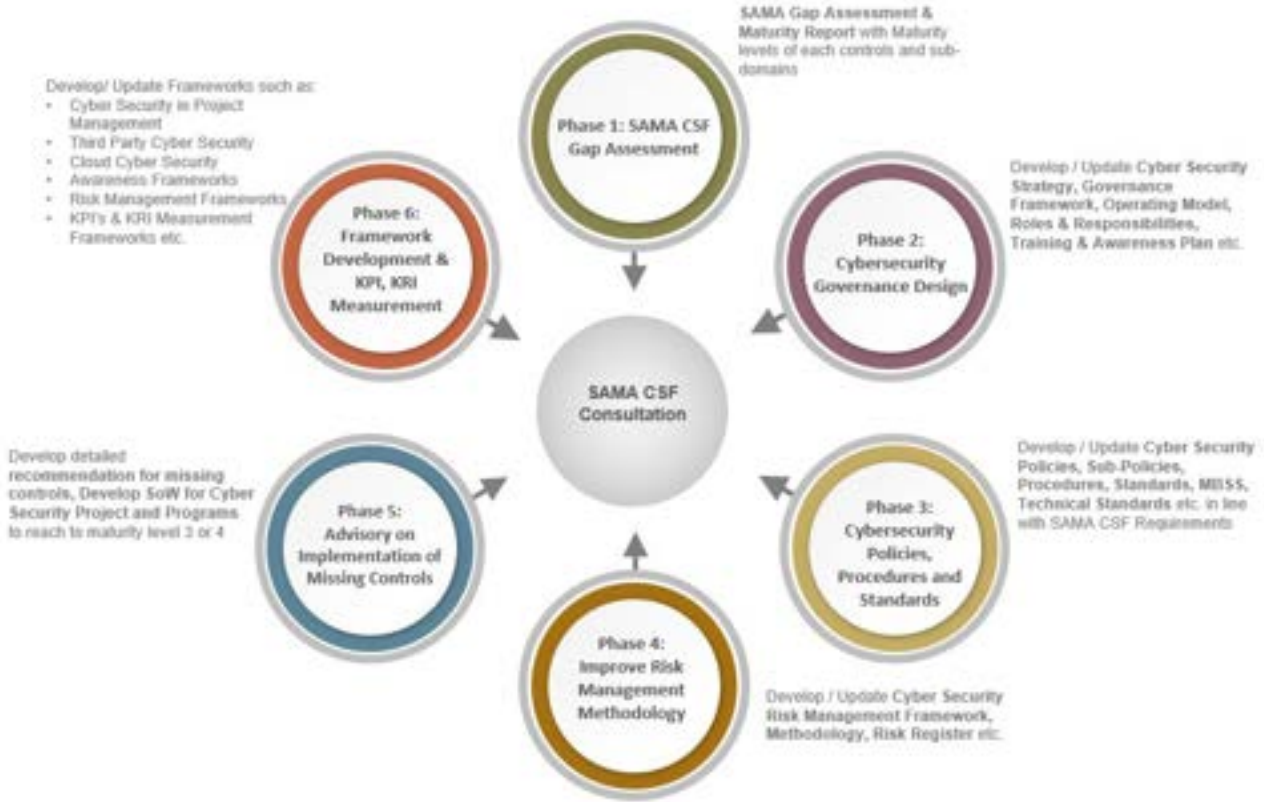
SAMA Cyber Security Maturity Model

The **Cyber Security Maturity Level** will be measured with the help of a predefined cyber security maturity model. The cyber security maturity model distinguishes 6 maturity levels (0, 1, 2, 3, 4 and 5), which are summarized in the table. In order to achieve levels 3, 4 or 5, a Member Organization must first meet all criteria of the preceding maturity levels.

Maturity Level	Definition and Criteria	Explanation
0 Non-existent	• No documentation. • There is no awareness or attention for certain cyber security control.	• Cyber security controls are not in place. There may be no awareness of the particular risk area or no current plans to implement such cyber security controls.
1 Ad-hoc	• Cyber security controls is not or partially defined. • Cyber security controls are performed in an inconsistent way. • Cyber security controls are not fully defined.	• Cyber security control design and execution varies by department or owner. • Cyber security control design may only partially mitigate the identified risk and execution may be inconsistent.
2 Repeatable but informal	• The execution of the cyber security control is • based on an informal and unwritten, though standardized, practice.	• Repeatable cyber security controls are in place. However, the control objectives and design are not formally defined or approved. • There is limited consideration for a structured review or testing of a control.
3 Structured and formalized	• Cyber security controls are defined, approved and implemented in a structured and formalized way. • The implementation of cyber security controls can be demonstrated.	• Cyber security policies, standards and procedures are established. • Compliance with cyber security documentation i.e., policies, standards and procedures is monitored, preferably using a governance, risk and compliance tool (GRC). • key performance indicators are defined, monitored and reported to evaluate the implementation.
4 Managed and measurable	• The effectiveness of the cyber security controls are periodically assessed and improved when necessary. • This periodic measurement, evaluations and opportunities for improvement are documented.	• Effectiveness of cyber security controls are measured and periodically evaluated. • key risk indicators and trend reporting are used to determine the effectiveness of the cyber security controls. • Results of measurement and evaluation are used to identify opportunities for improvement of the cyber security controls.
5 Adaptive	• Cyber security controls are subject to a continuous improvement plan.	• The enterprise-wide cyber security program focuses on continuous compliance, effectiveness and improvement of the cyber security controls. • Cyber security controls are integrated with enterprise risk management framework and practices. • Performance of cyber security controls are evaluated using peer and sector data.

Our Approach to SAMA CSF Readiness

Organizations in Saudi Arabia are required to reach, **Maturity level 3 or above**. With the designed approach, we help organisations in reaching the desired state, by performing the following phases.



Security Best Practices

databrackets

- Strong Passwords
- Install and Maintain Anti-Virus Software
- E-mail Best Practices
- Wireless Vulnerabilities
- Mobile Device Security
- Cloud-based Applications
- Social Media Engagement
- Electronic Data Disposal
- Remote Working
- Control Physical Access
- Plan for the Unexpected

Best Practices to secure private health data.

1. Strong Passwords

1. Minimum 8 Characters
2. Combination of upper and lower case
3. Change every 90 to 180 days with password recovery options

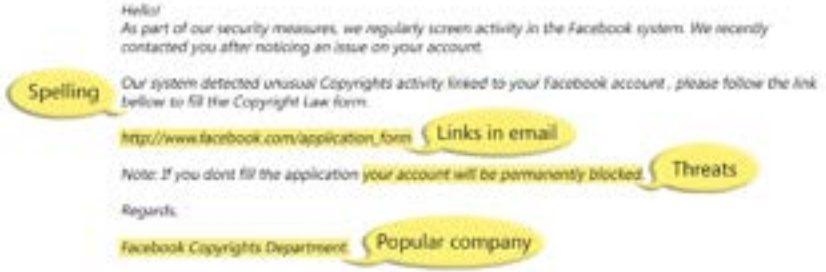
Do you use password managers to maintain passwords?

2. Install and Maintain Anti-Virus Software

1. Prevents unapproved software install
2. Protects against thumb drive and external media exploits
3. Must be kept up to date
4. Ensures real-time monitoring

Keep your AV up-to-date and never allow users to turn it off.

3. E-mail Best Practices



http://192.168.255.205/facebook/index.htm

1. Think before you act!
2. Clicking on the URL
3. Opening Attachments
4. Responding to a message
5. Limit sending sensitive data via e-mail

Scan all attachments via email service provider.

4. Wireless Vulnerabilities

- ✓ Unauthorized wireless technology
- ✓ Public Wi-Fi
- ✓ Lack of strong encryption
- ✓ Secure your home router
  - Default password
  - Up-to-date firmware

Ensure you have additional protections when using public Wi-Fi.

5. Mobile Device Security

- ✓ Easy to lose and vulnerable to theft
- ✓ Prone to data corruption
- ✓ Unauthorized access
  - Viewing of data
  - Access control
- ✓ Data encryption
- ✓ Any device handling customer data should be managed including all personal devices.

6. Cloud-based Applications

- ✓ **Public Clouds**
  - e.g., Gmail
- ✓ **Private Clouds**
  - Archiving of Images
  - On-line Backups
- ✓ **Community Clouds**
  - e.g., HIE
- ✓ **Hybrid Clouds**
  - e.g., Dropbox

Cloud computing that protects sensitive patient data via compliance safeguards.

7. Social Media

Never post any sensitive data on social media sites including pictures, videos, etc. without written permission from the subjects.

PHI is one of the most significant concerns related to social media.

8. Electronic Data Disposal

- ✓ Optical Media(CDs, DVDs)
- ✓ Shredder
- ✓ Magnetic media (hard drives, magnetic disks and tapes, removable memory cards, flash drives, floppy and ZIP disks, tapes, cartridges, etc.)
- ✓ Sanitization of magnetic data before disposal or physical destruction

Emptying the recycle bin is not enough.

9. Remote Working

- ✓ Ensure Physical Security
- ✓ Be aware of your surroundings and activities
- ✓ Use only secure network connection
- ✓ Virtual Private Network
- ✓ Ensure adequate encryption

Enable MFA for all system access.

10. Control Physical Access

- ✓ Single most common way of sensitive data compromise
- ✓ Restrict access/Visitor Logs
- ✓ Privacy screen

Ensure cameras are enabled on key locations.

11. Plan for the Unexpected

- ✓ Fire, flood, hurricane, earthquake and other natural or man-mad disasters
  - Creating backups
  - Having a sound recovery plan
  - Validating the plan

Business continuity testing is important.

Symptoms of a Breach [1/2]

1. Denial of service
2. Degraded network performance
3. Increased suspect events in system logs
4. Reports of ID theft from clients
5. Missing data storage devices

Check out for the leading cause of healthcare data breaches.

Symptoms of a Breach [2/2]

- ✓ Web page is defaced
- ✓ Increase of suspect e-mail traffic
- ✓ Presence/detection of Trojans/viruses/ malware
  - Business Network into spam bot
  - Command and control
  - Key loggers
- ✓ Suspicious or Unusual Login Activities

Check out for the leading cause of healthcare data breaches.

What Do You Do If You Suspect A Breach

- ✓ Inform your security officer
- ✓ Leave the device as-is to preserve the original copies
- ✓ Engage forensic examination
- ✓ Criminal investigation (FBI, State Law Enforcement)
- ✓ Notify concerned agencies
- ✓ Notify Media (If required)

Steps to take after a data breach.

Resources

- SAMA Cybersecurity Framework

  https://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf

- NIST guidance for Security Practice

  http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

- Security best practices for small practices

  http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Key Takeaways

- ✓ Increased enforcement & audits by government agencies
- ✓ Sensitive Data - Focus of all security and privacy programs
- ✓ Minimum Necessary Usage and Disclosure (Paper, electronic and verbal)
- ✓ There is no silver bullet to secure data - it is a journey of continuous internal improvement, training and awareness

Key Takeaways that emphasize the value and importance of protecting patient data.

FIND US

CALL US
866-276 8309

SERVICE
info@databrackets.com

LOCATION
150, Cornerstone Dr.
Cary, NC

SOCIALIZE
Facebook
Twitter

Twitter: @databrackets

Facebook: databrackets

databrackets
cybersecurity • audit • compliance

Thank You

for your attention!

databrackets
cybersecurity • audit • compliance