HELP! WE'VE BEEN HACKED…

Guidance on responding to a cybersecurity incident and managing the increasing risks of Cyber threats & Attacks;

Based on Legal and Risk perspectives in relation to Cybersecurity

Ms. Keisha M Durham

PARTNER
HEAD OF LEGAL
SAGE BVI

Mr. Nigel L
Massicot

PARTNER
HEAD OF LIQUIDATIONS &
RESTRUCTURING
SAGE BVI

INTRODUCTION

❑ Brief Introduction to Sage BVI and Partners presenting on this session

❑ Ms. Keisha M. Durham

Keisha M Durham, is a senior Partner and Director of Legal Services at Sage BVI: a blended practice firm in the British Virgin Islands offering a combination of legal, restructuring, accounting and consultancy services. Keisha is a Barrister of the Eastern Caribbean Supreme Court with extensive professional experience and expertise which she has gained from over 20 years practice to date. She specializes in Commercial & Civil Litigation, Corporate Governance, and is actively developing her expertise in Data Protection, risk management and laws relevant to Cybersecurity and AI . The quality and depth of Keisha's experience, enable her to provide effective legal perspective, strategy and representation in a manner that adds significant value to clients and teams.

❑ Mr. Nigel L. Massicot

Nigel L. Massicot, is a senior Partner and Head of Restructuring & Liquidations at Sage BVI: a blended practice firm in the British Virgin Islands offering a combination of legal, restructuring, accounting and consultancy services. He is also the firm's Director of Operations. Nigel is an Accountant by profession with extensive professional experience and expertise which he has developed over the past 20 years working in the financial services industry in the Virgin Islands (British). He specializes in the restructuring of corporate groups and entities particularly through the liquidation process.

❑ CYBERSECECURITY EXPERIENCE & PRACTICE

In 2021-20222, Nigel & Keisha co-lead Sage BVI's team through its first formal Cybersecurity Review & Assessment, independently verified by a leading cyber risk management organization based in Colorado, which provides analytics and verifies cybersecurity resilience for a large number of companies. This assessment confirmed Sage BVI's compliance with international standards in relation to Cybersecurity. Nigel coordinated the implementation of data security protocols and policies required to ensure Sage BVI's compliance with international standards and best practice in relation to Cybersecurity. Keisha was responsible for drafting and updating policies to ensure Sage BVI's compliance with standards and ISOs in relation to Cybersecurity, as well as managing risks in this regard.

CYBER SECURITY : KEY TERMS

CYBERSECURITY : commonly used term oftentimes improperly/ inadequately defined. We have found that a useful definition from McKinsey & Co:

“It’s what organizations do to protect their own and their customers’ data from malicious attacks.”

CYBERSECURITY EVENT

Any observable occurrence in a system, network, environment, process, workflow, or personnel. Events may or may not be negative in nature.
ADVERSE EVENTS: are those with negative consequences

CYBERSECURITY INCIDENT

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations.

CYBERSECURITY ATTACK

Any malicious attack on a computer system, network, or device to gain access and information. There are **many different types of cyberattacks**.
HACKING is a catch all term often used to describe a Cybersecurity attack and essentially means the same thing. Here are some of the most common ones:

CYBER SECURITY ATTACKS

HERE ARE SOME OF THE MOST COMMON TYPES OF CYBER ATTACKS
(not an exhaustive list as threat/ attack landscape changes)

PHISHING (#1 ranked by FBI)

Phishing involves a bad actor sending a fraudulent message that appears to come from a legitimate source, like a bank or a company, or from somebody with the wrong number. Phishing attacks are made through email, text, or social networks.

DENIAL OF SERVICE ATTACKS

Denial-of-service attacks flood systems with traffic to clog up bandwidth so that they can't fulfill legitimate requests. The goal of this type of attack is to shut down systems.

MALWARE

MALWARE is malicious software, including spyware, ransomware, and viruses. It accesses a network through a weakness—for example, when a member of the network clicks on a fraudulent link or email attachment.

PASSWORD ATTACKS

Password attacks are mounted by cybercriminals who try to steal passwords by guesswork or trickery.

MAN IN THE MIDDLE ATTACKS

These are incidents in which an attacker comes between two members of a transaction to eavesdrop on personal information. These attacks are particularly common on public Wi-Fi networks, which can be easily hacked.

SO, You have been HACKED!

HOW NOT TO RESPOND…

BEFORE we discuss BEST PRACTICES, it is important to know HOW NOT TO RESPOND so that you know what type of reactions to guard against when facing a Cybersecurity Incident that triggers panic, uncertainty, embarrassment etc.

#1: DO NOT BE SLOW TO REACT

A slowed and thus delayed reaction and response often happens where you and your organization/ firm are unprepared. With no incident response & management plan already in place it takes far too long to **properly react** to the incident. As a result there can be seriously damaging outcomes to your organization, practice and reputation.

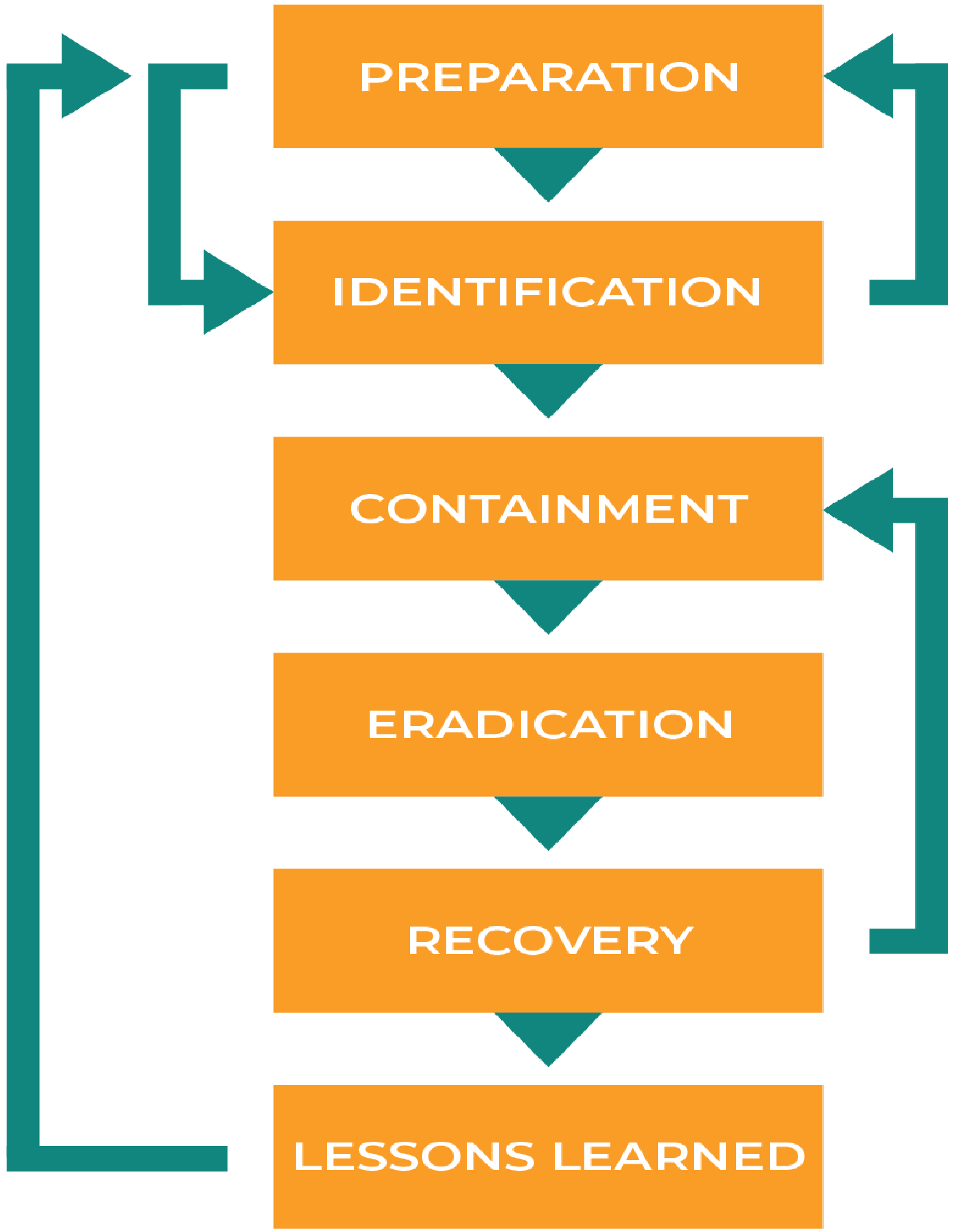
#2: RESPONDING/ REACTING TOO QUICKLY

If you are unprepared (in whole or in part) you could find yourself having a knee-jerk reaction. A common example of would be by shutting down IT operations. If this happens, or you advise that this step be taken and your firm acts in this way, critical evidence could be accidentally deleted r; OR there could be damage caused to IT assets and Data that you could have recovered.

#3: FAILURE TO CO-ORDINATE

Oftentimes expectations, priorities, and channels of communication are not properly managed in a crisis situation, as a result, there would be inconsistency in language and/or action, lack of reporting to seniors and/or experts who are critical to decision making, thus compounding & deepening the crisis as response times and decisions become adversely affected.

CYBER SECURITY INCIDENT RESPONSE FRAMEWORK



BASED ON PICERL FRAMEWORK MODEL

PHASE 01 : PREPARATION

It is essential to establish a Cyber Security Incident Response Team (CSIRT), define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools.

PHASE 02: IDENTIFICATION

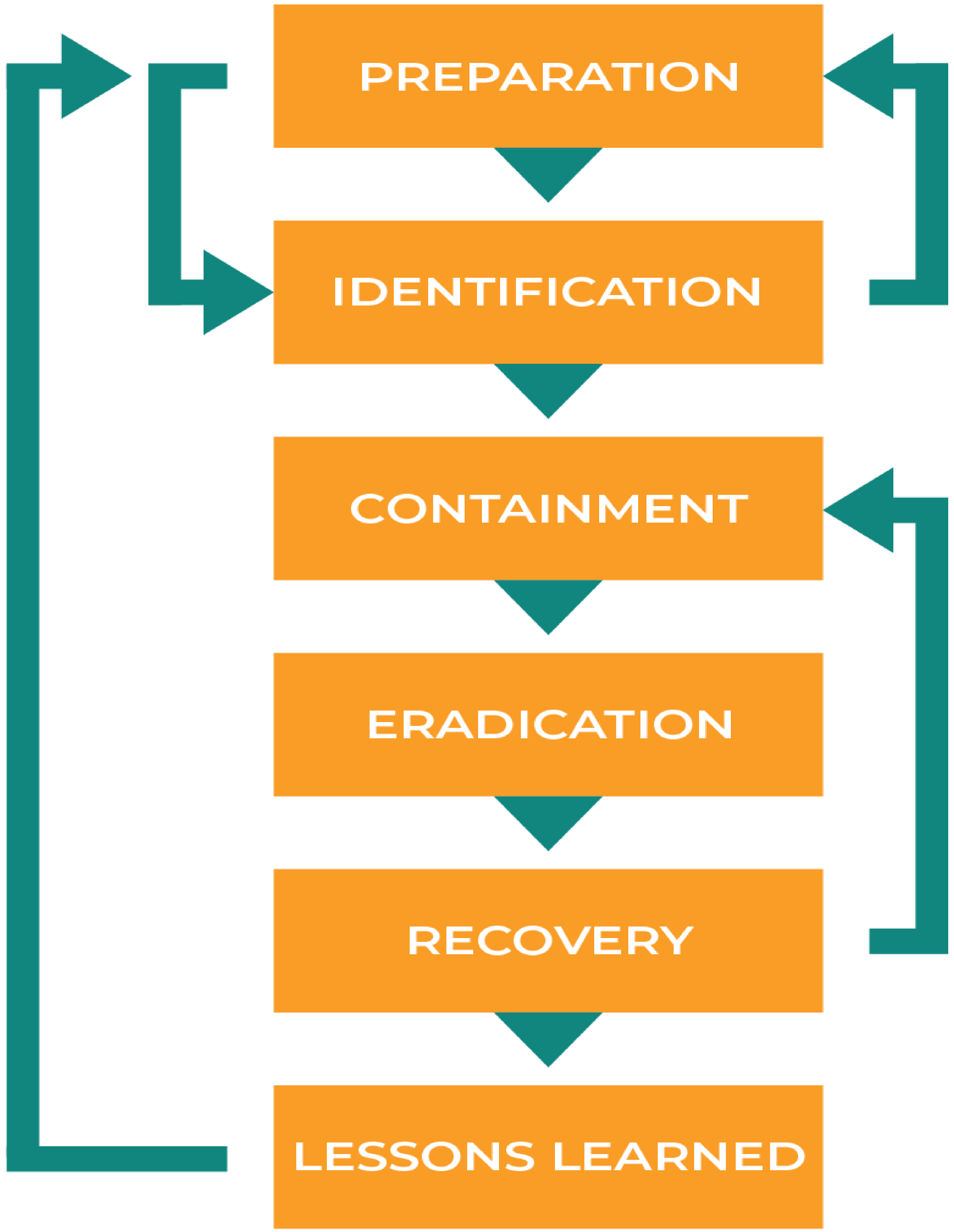
Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legislative and legal requirements.

PHASE 03: CONTAINMENT

Containment of the incident is necessary to minimize and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties.

CYBER SECURITY INCIDENT RESPONSE FRAMEWORK

Based on PICERL Framework Model



PHASE 04 : ERADICATION

Eradication requires removal or addressing of all components and symptoms of the incident. Further, validation must be performed to ensure the incident does not reoccur.

PHASE 05: RECOVERY

Recovery involves the steps required to restore data and systems to a healthy working state allowing business operations to be returned.

PHASE 06: LESSONS LEARNED

The Lessons Learned phase includes post-incident analysis on the system(s) that were impacted by the incident and other potentially vulnerable systems. Lessons learned from the incident are communicated to executive management and action plans developed to improve future incident management practices and reduce risk exposure.

Managing increased risks of Cyberattacks & Threats:

What can organizations do to mitigate future threats

Zero-trust architecture (ZTA). In this security system design, all entities—inside a
outside the organization’s computer network—are not trusted by default and mu
their trustworthiness. ZTA shifts the focus of cyberdefense away from the static p
around physical networks and toward users, assets, and resources, thus mitigatin
from decentralized data.

Behavioral analytics. These tools can monitor employee access requests or the
devices and identify anomalous user behavior or device activity.

**Building, Maintaining & Fostering a strong internal cybersecurity culture withi
organization / firm or team** : Any organization or team is only as good as its peo
security is only as strong as their understanding of why security matters.

**Adopt a cybersecurity focused approach to human resources both in the hiring
continuous development of your team:** Technical controls and capabilities are, a
always be, necessary to secure the environment of any organization. But it will b
better positioned to reduce its exposure to cybersecurity risk if it adopts a new a
hiring cybersecurity talent. That approach focuses on preplanning and understan
cybersecurity needs holistically.

What is Cyber Risk?

Cyber risk is a form of business risk, with potential for business losses of all kinds, not only in the digital domain but also financial, reputational, operational, productivity related, and regulatory related.

Cyber Threats vs. Cyber Risk

Cyber risk is not the same as a cyberthreat.

Cyberthreats are the particular dangers that create the potential for cyber risk.

These include: privilege escalation vulnerability exploitation, or phishing.

Cyber Security Approaches

Maturity-Based Approach

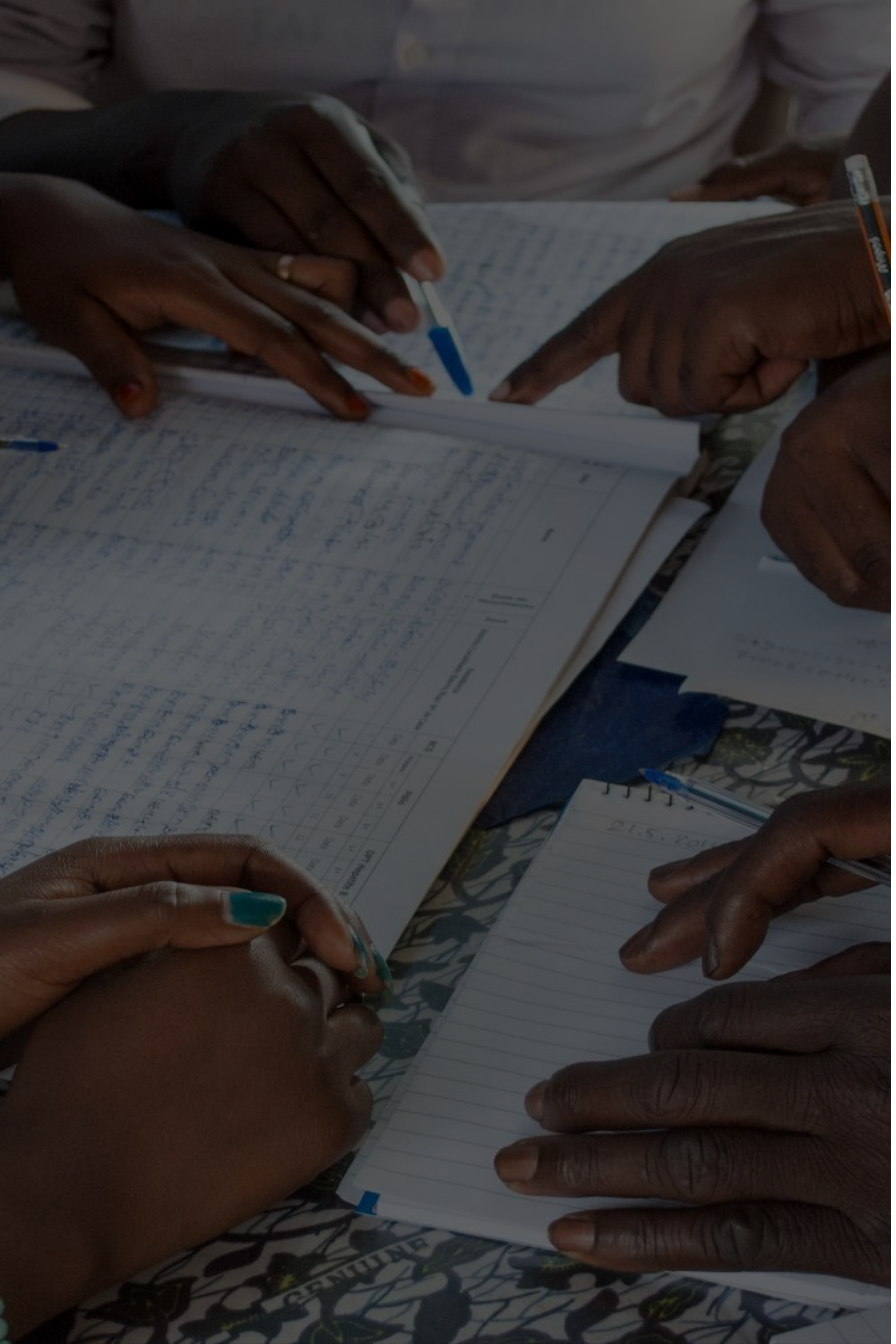
Vs.

Risk Based Approach

Cyber-Security Risk-based Approach

A risk-based approach identifies risk reduction as the primary goal.

A risk-based approach breaks down risk-reduction targets into precise implementation programs with clear alignment all the way up and down an organization



Risk-based Cybersecurity Approach

There are eight actions that comprise a best practice for developing a risk-based cybersecurity approach:

1. fully embed cybersecurity in the enterprise
2. define the sources of enterprise value across teams, processes, and technologies
3. understand the organization’s enterprise-wide vulnerabilities—among people, processes, and technology—internally and for third parties
4. understand the relevant “threat actors,” their capabilities, and their intent
5. link the controls in “run” activities and “change” programs to the vulnerabilities that they address and determine what new efforts are needed
6. map the enterprise risks from the enterprise-risk-management framework
7. plot risks against the enterprise-risk appetite
8. monitor risks and cyber efforts against risk appetite, key cyber risk indicators, and key performance indicators

CONCLUSION

❑ **TAKEAWAYS:**

❑ **LESSONS LEARNED FROM COMPANIES/ ORGANISATIONS WHO FACED & RECOVERED FROM CYBER SECURITY ATTACKS/ CRISES:**

Quotes from Julia Houston, chief strategy and marketing officer at Equifax Inc., on how the credit bureau managed one of the biggest data breaches in history

❑ **WILLINGNESS TO CHANGE**

E#ective change management is one of the most underrated tools in corporate America," "You've got to set the tone at the top, but executives can't just decide they're going to change and expect everybody in the organization to adapt. You've got to get all your thousands of employees on board and manage that change all the way down through the organization."

❑ **INVEST IN THE TOOLS & INFRASTRUCTURE NEEDED**

"Once you've been through a crisis of the magnitude that we experienced, it fortunately doesn't take a lot of convincing to make an investment in resilience," Houston said, adding, "I like to say that we followed Winston Churchill's admonitions to never let a good crisis go to waste."

❑ **CONTINUOUS IMPROVEMENT, LEARNING & DEVELOPMENT**

❑ **ONGOING MONITORING OF YOUR CYBER ENVIRONMENT, CYBER HYGIENE & CYBER SECURITY**