March 2, 2022

A cyber panel on

Incident Response & Readiness

tcdi

Steven Wujek

Network Architect
& Security Engineer

Michael Best

Joseph Dickinson

Partner @ Michael
Best & Fredrich LLP

ONE SOURCE

Steve Cobb

Chief Information
Security Officer

Atticus

Ben Hopf

Founder & CEO

COMING IN HOT 🔥

Agenda

ESTABLISH AN UNDERSTANDING

Incident Response Plans— What it is, what to expect (or look for) within, and the reasons you must have one

STAGES OF THE LIFE CYCLE

A breakdown of the NIST and SANS incident response steps and what an actual incident feels like

EXPERT TIPS & SUGGESTIONS

A crash course in what to do & what not to do, including examples of our hardest-learned lessons

CURRENT TRENDS & OBSERVATIONS

Let's be honest... this "new normal" deserves some candid tech advice for thriving vs. merely surviving

Everything you need to know about

Incident Response & Readiness Plans

Trust Advisors Forum
March 2, 2022

WHAT IS AN—

Incident Response Plan

An Incident Response Plan is a set of documented procedures detailing the steps that should be taken in each phase of incident response. It should include guidelines for roles and responsibilities, communication plans, and standardized response protocols.

LEARN MORE

TIP: Feel free to use this template as a base, and modify it to suit your organization's specifics. Just delete these text boxes when you're done.

Incident Response Plan

Author: [Your company name] Inc.

Version: 1.x

01

02

04

06

GOAL: SYSTEMS NORMAL

ESTABLISHING AN UNDERSTANDING

7 reasons you need an IRP

01 **Prepares you for an emergency**—

security incidents happen without warning, so it’s essential to prepare a process ahead of time

02 **Repeatable process**—

Without an incident response plan, teams cannot respond in a repeatable manner or prioritize their time

03 **Coordination**—

In large organizations, it can be hard to keep everyone in the loop during a crisis… an IRP can help ensure this

04 **Expose gaps**—

Advanced planning can expose obvious gaps in the security systems or processes and help address them *beforehand*

05 **Preserves critical knowledge**—

Ensures best practices for dealing with a crisis aren’t forgotten over time & that learned lessons are incrementally added

06 **Practice makes perfect**—

Plans create a clear, repeatable process that can be coordinated, followed & improved in effectiveness over time

07 **Documentation and accountability**—

Clear documentation reduces an org’s liability by being able to demonstrate to auditors & authorities what was done to prevent breach

ESTABLISHING AN UNDERSTANDING

Plan readiness

Anatomy of an sound plan

- Purpose and Scope
- Preparation
- Roles and Responsibilities
- Response Procedures
- Playbooks

SKILLS ASSESSMENT

MILLION DOLLAR POP QUIZ

Who to contact first?

Trick question

WHEN TO CONTACT LEGAL?

WHEN TO CONTACT INSURANCE?

ESTABLISHING AN UNDERSTANDING

How to prepare

LEGAL ASPECTS

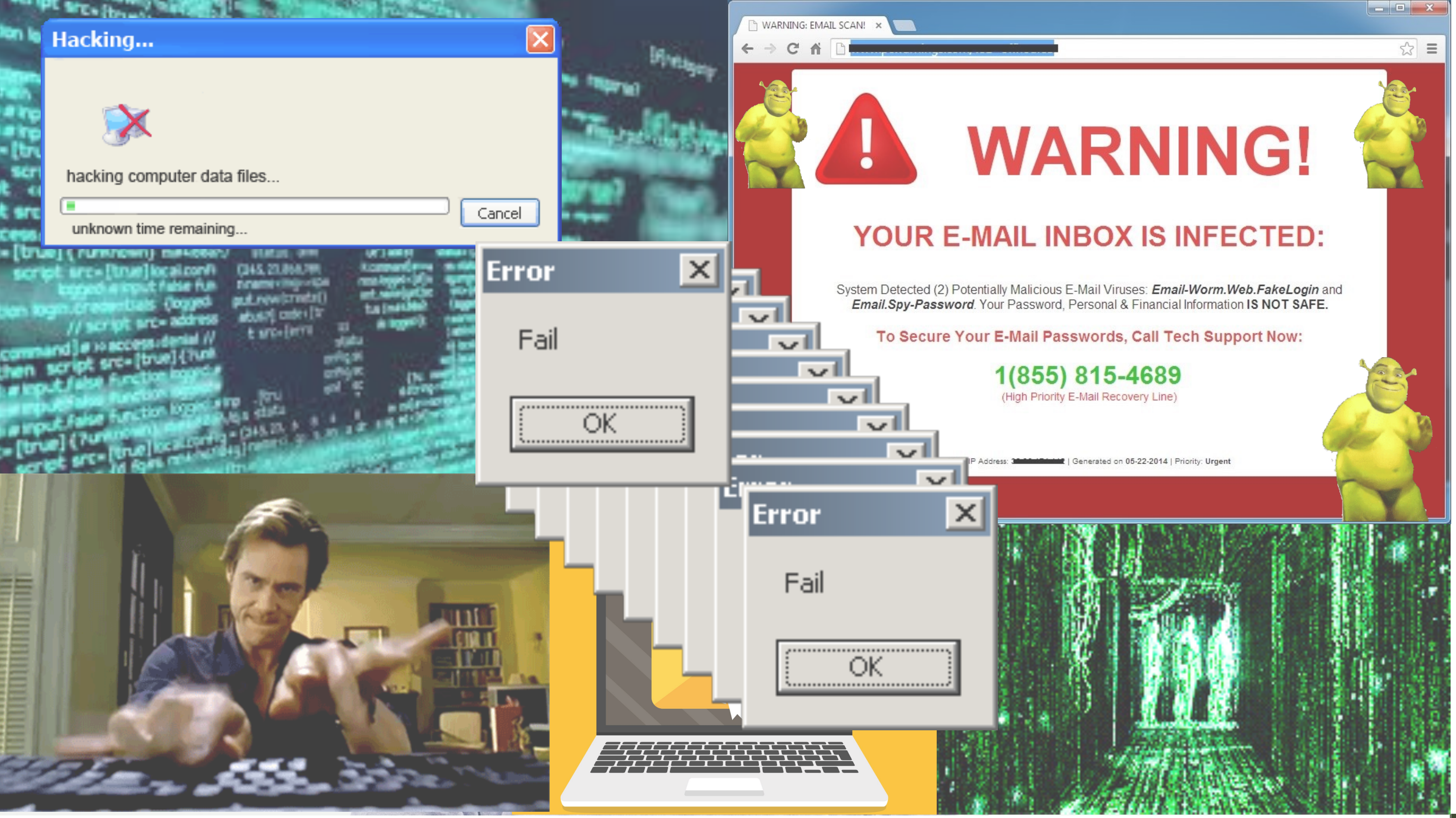
- Contractual requirements of clients?
- Obligations of vendors?
- Compliance Laws & Regulations
  (HIPPA, PCI-DSS, FDIC…)
- Other legal pitfalls & things to avoid

CYBER INSURANCE ASPECTS

- Appropriate coverage amounts?
- Reputation of Insurers
- Policy limits & allowances
  (HIPPA, PCI-DSS, FDIC…)
- Frequent plan to review & update/upgrade?

let’s set the stage

What does an incident life cycle feel like?


Hacking...
hacking computer data files...
unknown time remaining...
Cancel
Error
Fail
OK
WARNING: EMAIL SCAN!
[redacted]
WARNING!
YOUR E-MAIL INBOX IS INFECTED:
System Detected (2) Potentially Malicious E-Mail Viruses: Email-Worm.Web.FakeLogin and Email.Spy-Password. Your Password, Personal & Financial Information IS NOT SAFE.
To Secure Your E-Mail Passwords, Call Tech Support Now:
1(855) 815-4689
(High Priority E-Mail Recovery Line)
IP Address: [redacted] | Generated on 05-22-2014 | Priority: Urgent
Error
Fail
OK

SEND AN 🆘 TO THE WORLD

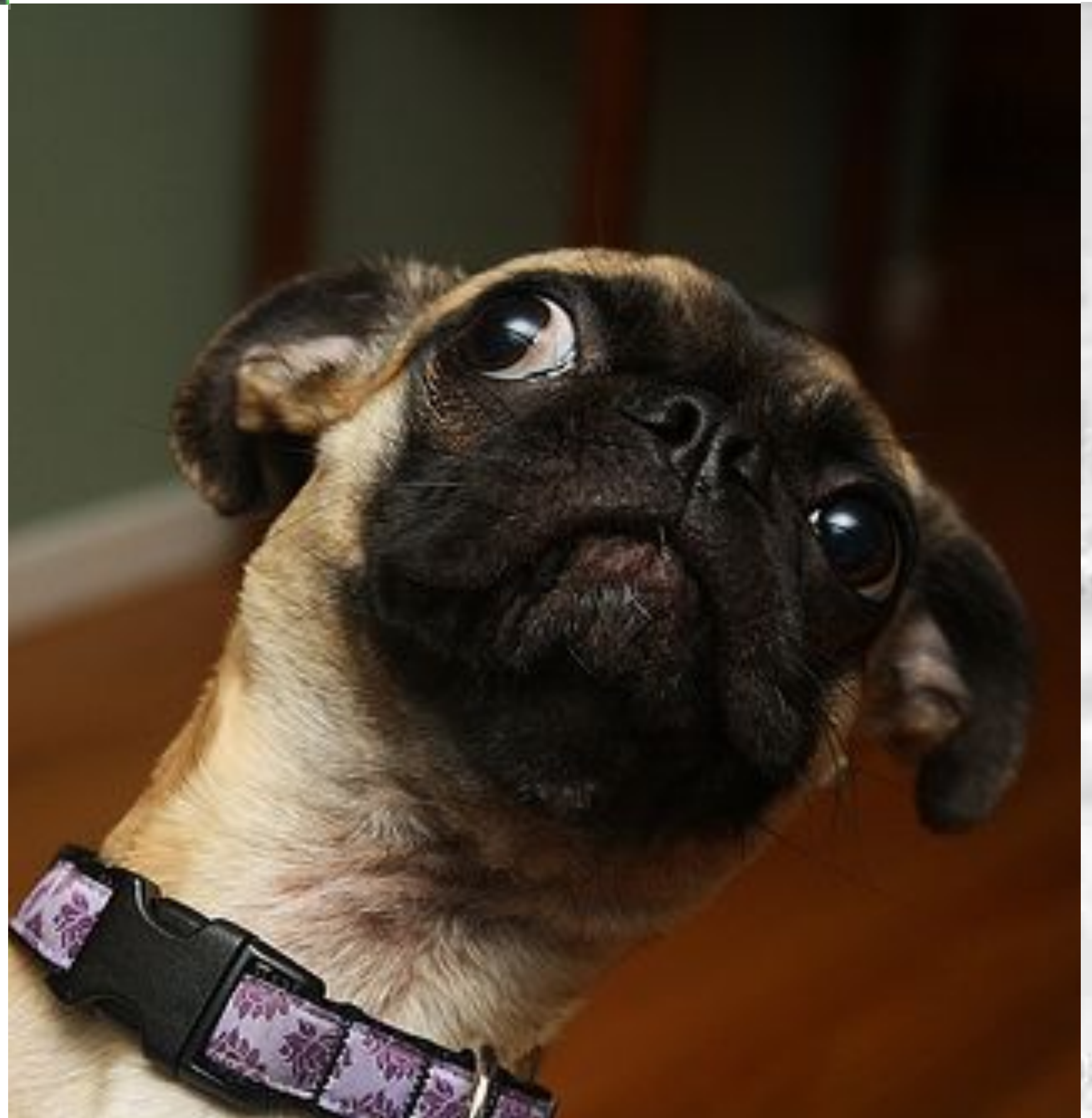
What you see

It's Monday morning, you walk in and everyone is looking at each other like Zombies. Confusion.. panic… Sales teams are all screaming.. your largest client just called to say they can't access their funds 😳…

SEND AN 🆘 TO THE WORLD

What we see

Nobody seems in charge. Nobody knows where the "Network Guy" is. The CTO is on vacation. CEO is teeing up on Pinehurst #2 with the CEO of your parent company. And some Sales guy keeps running up to me mumbling "I have a billion dollar deal I have to close this morning! When will the Network be back online?!?" 😳



the life cycle

of effective Incident Response Planning

STAGES OF THE LIFE CYCLE

Incident response steps

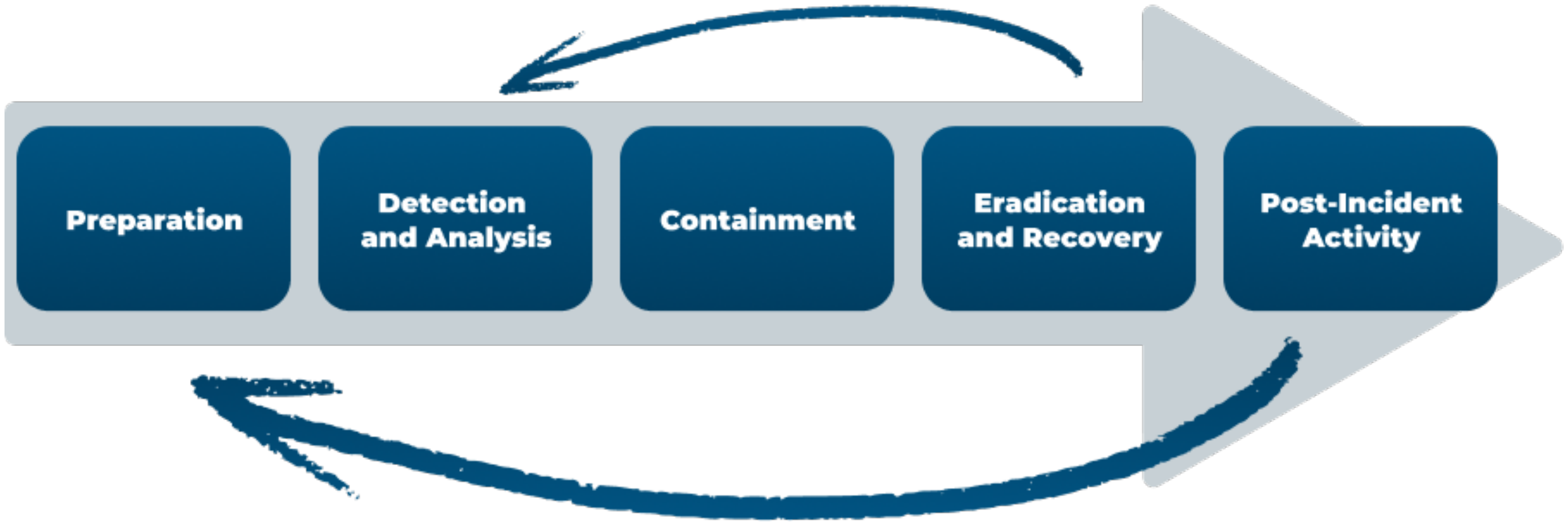
SANS

1) Preparation
2) Identification
3) Containment
4) Eradication
5) Recovery
6) Lessons Learned

NIST

1) Preparation
2) Detection and Analysis
3) Containment, Eradication& Recovery
4) Post-Incident Activity

CISCO



INCIDENT RESPONSE

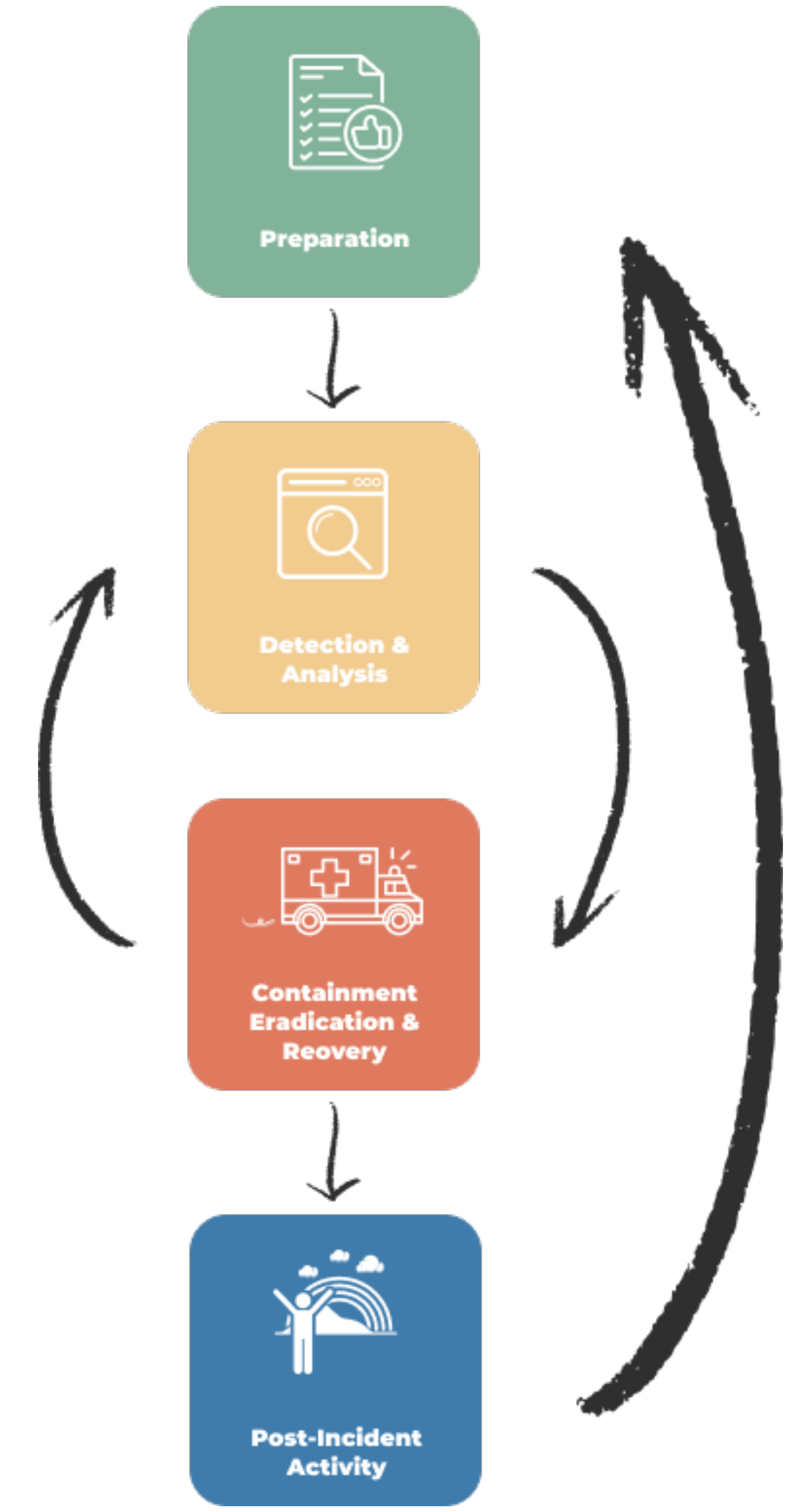
4 STAGES OF LIFE CYCLE

Normal

Beforehand 😎

BEFORE the incident has happened, focus on:

- Assessing different risks before they happen
- Establish ‘baseline’ for all protections
- Planning
- Training
- Monitoring



Preparation

Detection & Analysis

Containment Eradication & Reovery

Post-Incident Activity

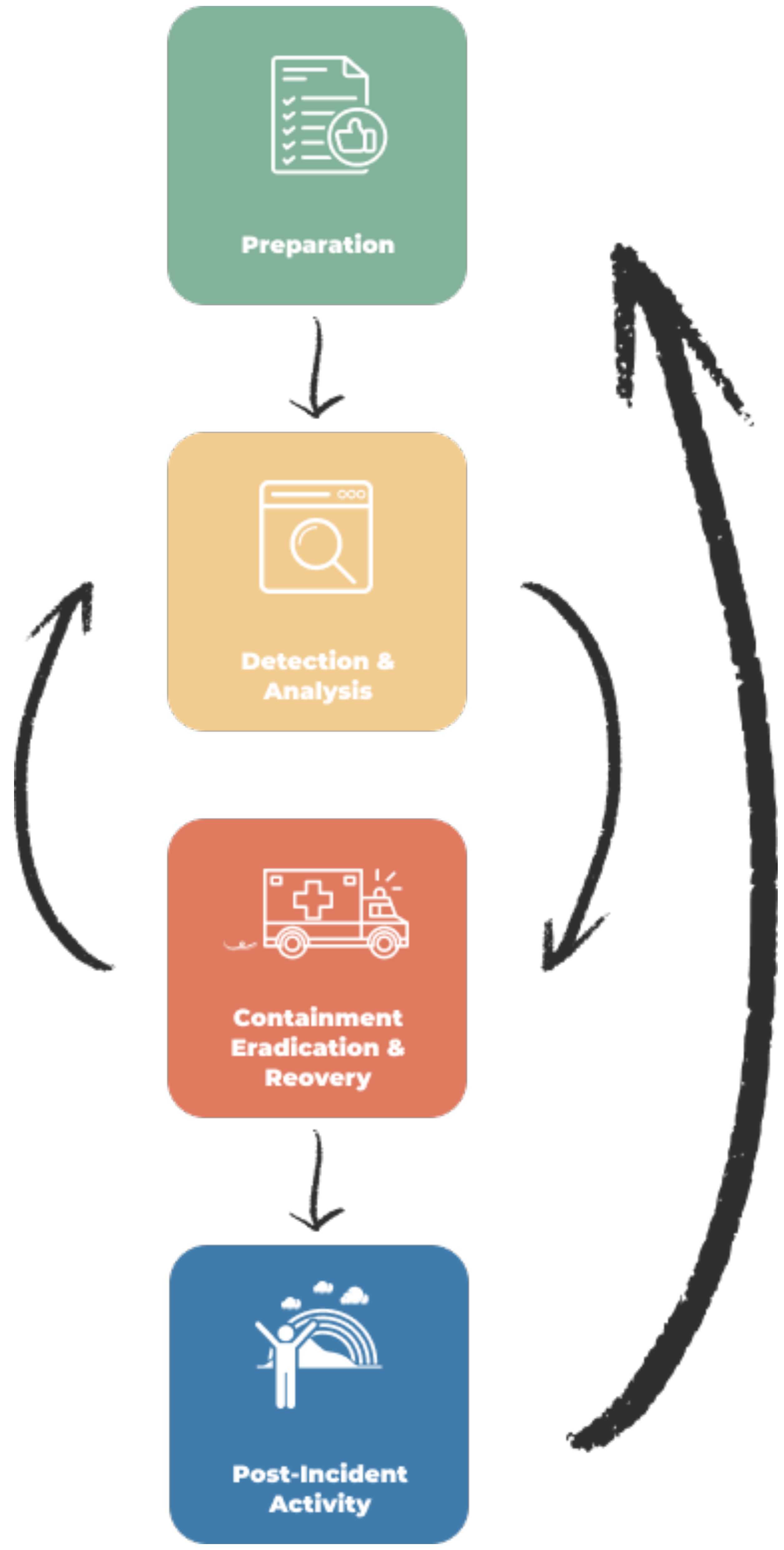
INCIDENT RESPONSE

4 STAGES OF LIFE CYCLE

Reported ⚠️

once an incident has been REPORTED, focus on:

- What [exactly] has happened?
- What has caused it?
- Validate it
- Document it
- What's our priority?
- Is it reportable?



Preparation

Detection & Analysis

Containment Eradication & Reovery

Post-Incident Activity

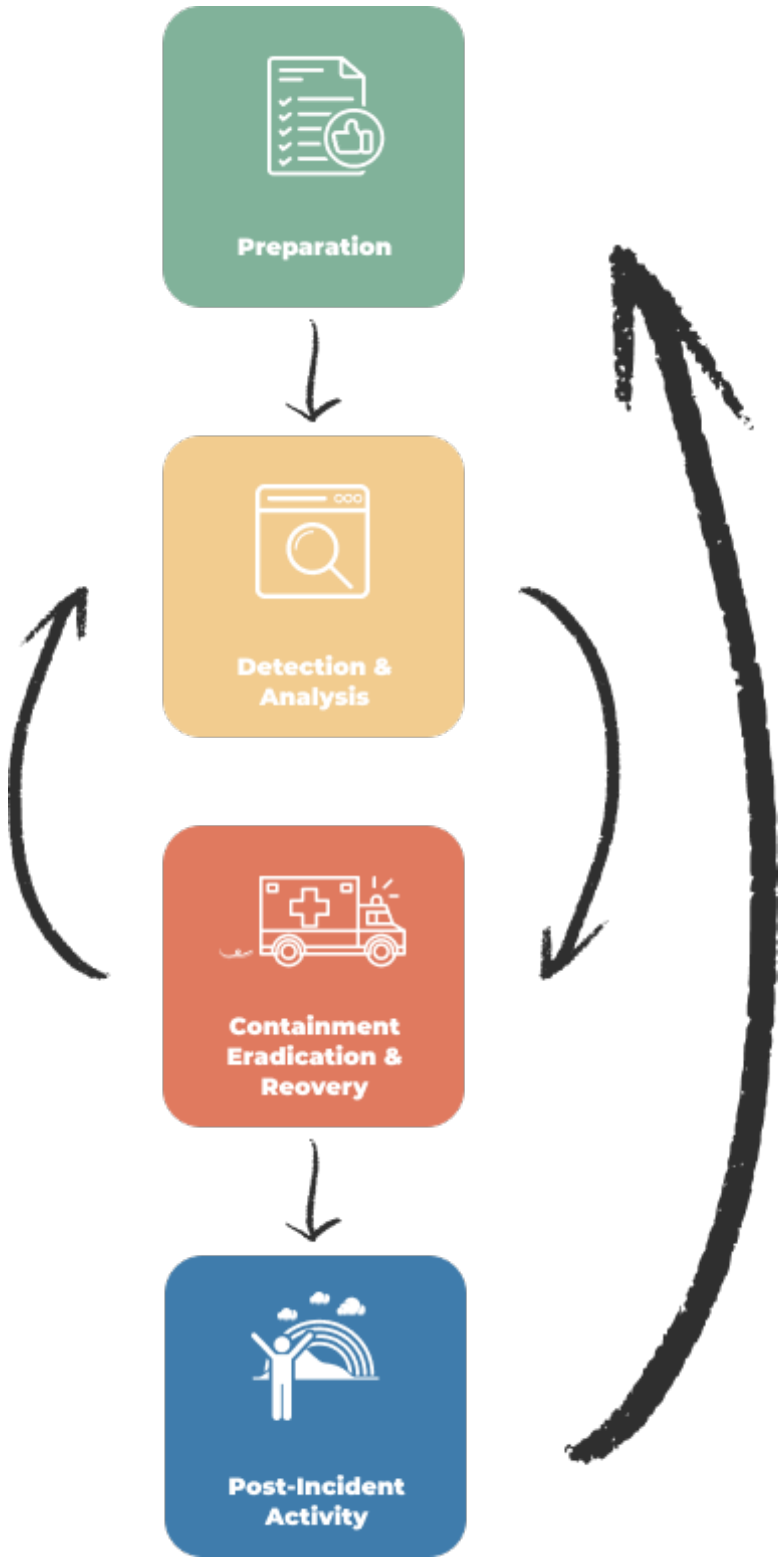
INCIDENT RESPONSE

4 STAGES OF LIFE CYCLE

Verified 💥

once an incident has been REPORTED, focus on:

- What [exactly] has happened?
- What has caused it?
- Validate it
- Document it
- What’s our priority?
- Is it reportable?



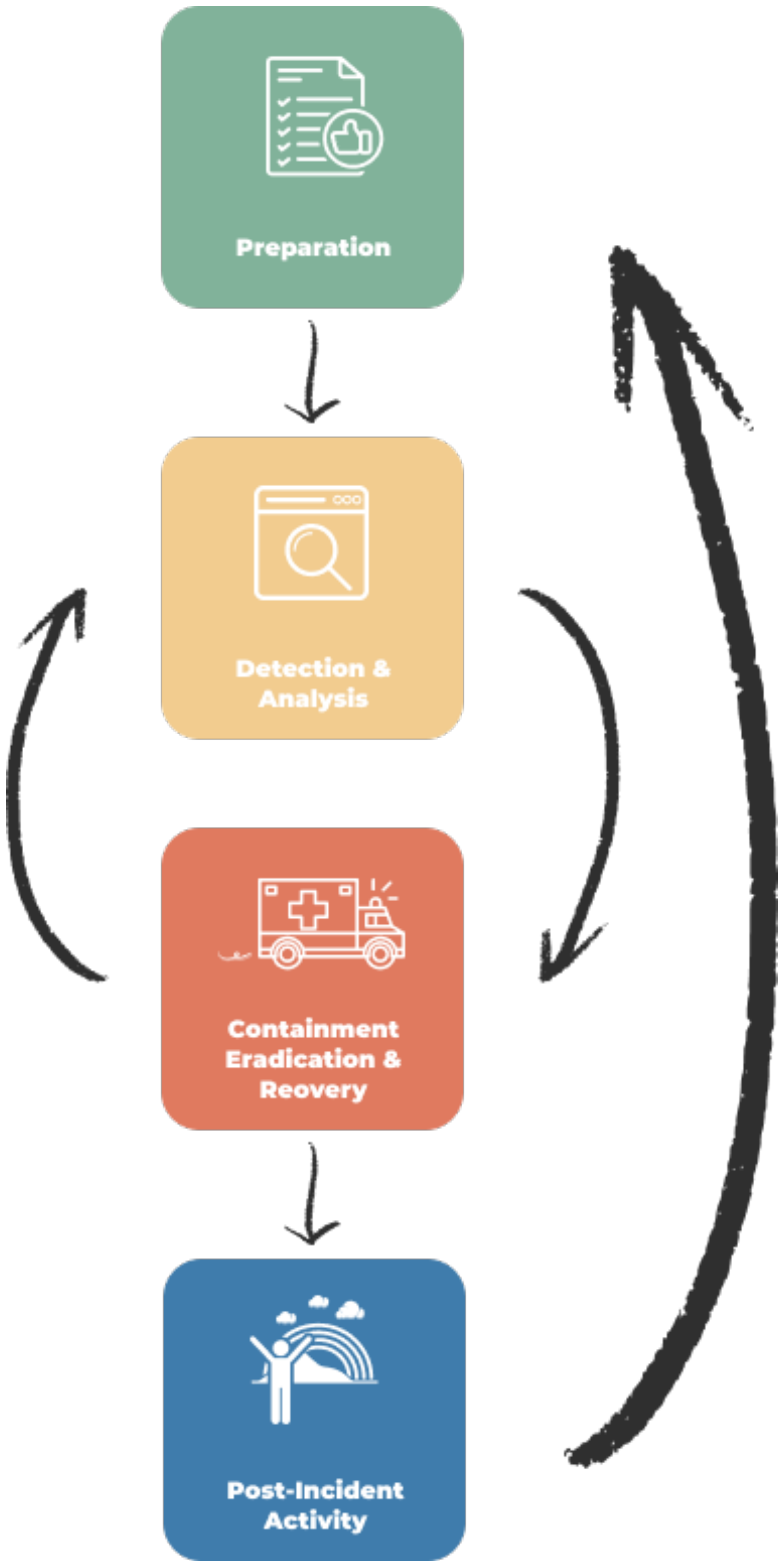
INCIDENT RESPONSE

4 STAGES OF LIFE CYCLE

Afterwards 🌀

AFTER the incident has happened, focus on:

- Follow-up reporting
- Document lessons learned
- Share learnings
- Update plan
- Continued prep & monitoring



tips & suggestions

for Incident Response Planning

PRO TIPS

Key Do's and Don'ts

- ✗ **DO NOT** call it a breach unless you know it's an actual breach
- ✓ **DO** involve outside counsel early *(but not too early)*
- ✓ **DO** know your regulatory and contractual notification requirements
- ✓ **DO** know if and when to engage law enforcement
- ✓ **DO** centralize communications
- ✓ **DO** assess the need, role and necessary coverage of insurance ahead of time
- ✓ **DO** test your plan regularly

PRO TIPS

Major mistakes to avoid

- 🤯 Not contacting IT Team first! *(Network Engineer, Systems Engineer, CISO)*
- 🤨 Calling your lawyer or legal team first… huh? (we see this a lot)
- 🫢 IT Team forgets to disable the wireless networks, allowing continued spread of infection
- 🤔 IT Team members can’t get into the Data Center or network closet to disconnect hardware/software
- 😫 IR responders don’t have a physical key for locked areas. *(Ask Steven about the network that burned!)*
- 🧐 IR responders (usually IT Team) don’t know where key network resources are located.

  Cloud? Data Center? Some other building? Some other State?
- 😡 Hounding the IR responders while they try to stop the infection.

  (Ask Steven about the manager who demanded updates every 5 minutes!)

current trends

regarding Incident Response Planning

CURRENT TRENDS

Security in today’s environment

- **Covid-10, work from home, remote access & new “virtual” normal**

  WFH & remote access opens an entirely different ballgame for compliance & security planning. This accelerated/forced digitization of certain technologies & industries appears to be permanent.

- **Increase in new vendors & technologies**

  Cloud-based. Regulatory globalization. Blockchain. Fintech primitives disrupting traditional bank tech stacks

- **Mega surge of micro-hackers & digital natives**

  Hacking used to be calculated, group-based & focused towards large companies. Now it’s just.. rampant

- **Insurance dilemmas**

  Companies getting dropped, prices going up as incidents (and payouts) more likely, etc

- **Geopolitical & Cyber-warfare: Ukraine & Russia**

appendix

Some extra resources to take back to your team or office…

Appendix 1

SOME EXTRA GOODIES

What to include in your IR plan

Essentials

- ✓ Phone numbers of all **IR Responders** on IT team
- ✓ **Direct contact info** for Department Heads and Managers
- ✓ Contact info of **Cybersecurity Vendor**
- ✓ Who to call internally, when to call, & **appropriate order** *(primary, secondary, etc.)*
- ✓ List of what to say (and what **not** to say)!
- ✓ List of **who to contact** at Cloud Vendors or 3rd party Partners
- ✓ Contact info for **CyberInsurance vendor** and **Legal Counsel**
- ✓ Appropriate emergency/non-emergency for **law enforcement**, FBI

Appendix 2

SOME EXTRA GOODIES

IR Tabletop Exercise

PRACTICE, PRACTICE …

… AND MORE PRACTICE

- ✓ Get a group together to practice
- ✓ Always cross-train by including other Departments

Appendix 3

SOME EXTRA GOODIES

🏴‍☠️ IR Tabletop Exercises

WHAT EXACTLY SHOULD WE PRACTICE?

- ⁉ Where is the Incident Response Plan? Is it printed or digital?
- ⁉ Who do you call and in what order? IT knows who to call, what about every other department?
- ⁉ Who’s going to "run point” for each specific type of incident?
- ⁉ Practice exercising ‘containment’ of the incident
- ⁉ Practice ‘stopping the bleeding/spread’…

Appendix 4

SOME EXTRA GOODIES

🏴‍☠️ IR Tabletop Exercises

DIFFERENT SCENARIOS TO PRACTICE:

- 🚨 What if ransomware hit an accountant’s desktop; how do we isolate Accounting?
- 🚨 West building hit by ransomware. How do we cut it off immediately, where’s the connection?
- 🚨 Tech Support just called you and reported what looks like ransomware at front of the building on a user’s laptop. Where is the network switch that controls that section so it can be unplugged?
- 🚨 A ransomware/virus is spreading. Who turns off the wireless access to prevent laptops from spreading it further? Who pulls the plug on the network switch?
- 🚨 An Accountant just wired $250,000 to a bogus company in Venezuela. Who do we call? How do we stop the transaction?

Appendix 5

SOME EXTRA GOODIES

Tips for every IT team

1. FIX THE BASICS

- **AntiVirus Software**— No freeware & run AV on everything. Prefer AV with AI built-in; XDR, EDR, Intelligence
- **Patching**— Patch everything and preferably set to ‘auto-update.’ Mean time to patch a system has shrunk down to minutes for many areas of IT.
- **Firewalls**— Software under a year old, and buy the security add-ons laptop. Where is the network switch that controls that section so it can be unplugged?
- **Backups**— Follow the 3-2-1 rule: 3x copies on 2x different backup formats, with at least 1x copy saved in the Cloud or offsite.

PSA: If your business has some fancy-schmancy ‘Digital Transformation’ initiative and you have us show up to help you deal with an ‘Incident’ and we find out your firewall(s) are 12 years old.... DON’T be that company! 🤦‍♂️

Appendix 6

SOME EXTRA GOODIES

Tips for every IT team

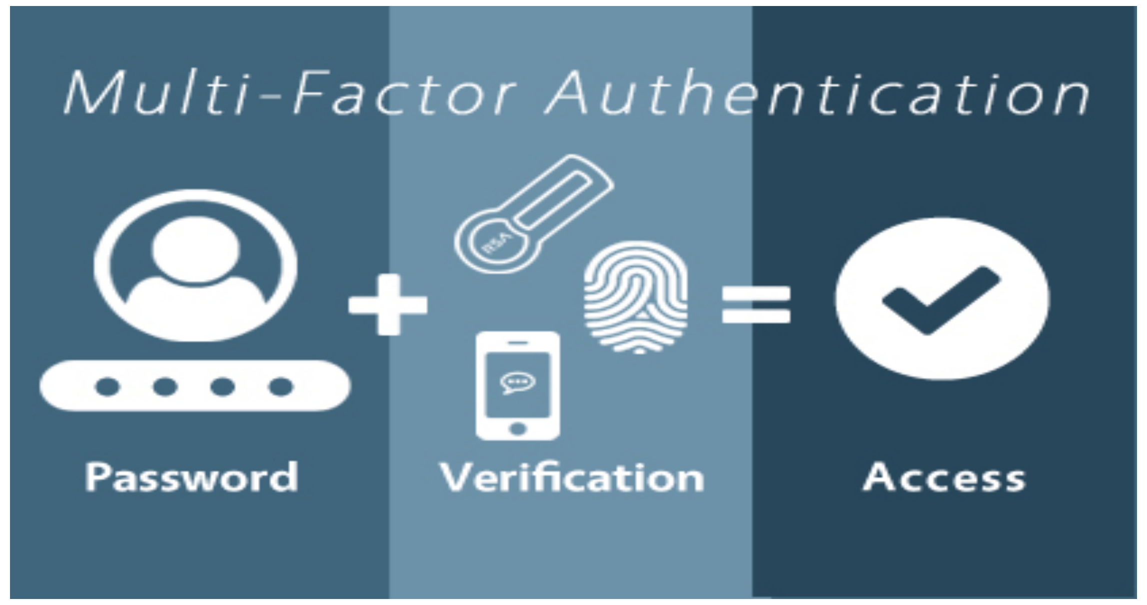
2. USE MULTI-FACTOR AUTHENTICATION EVERYWHERE!

If there is one factor that has stopped the majority of hacks better than any other tactic we've seen recently, it's a solid MFA solution!

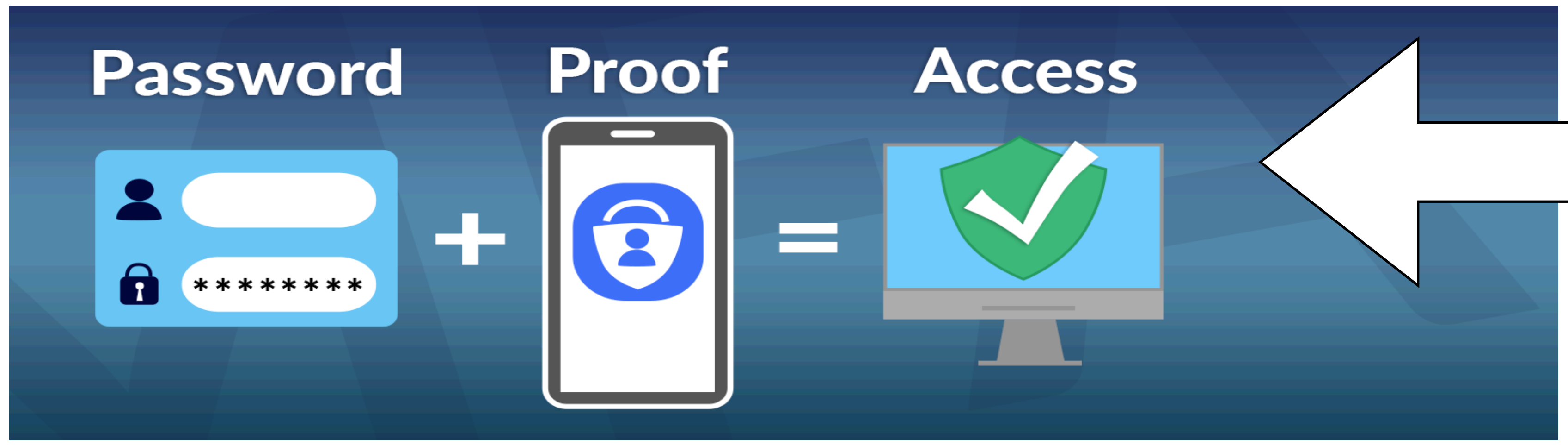
Some vendors you may recognize:

- DUO
- Okta
- Yubikeys
- PingID
- DoubleOctopus
- RSA

⭐ Use MFA on all accounts!!! ⭐



What is MFA ??
Multi-factor authentication (MFA) is a security technology that requires multiple methods of authentication to provide an extra layer of protection on top of standard username & passwords.



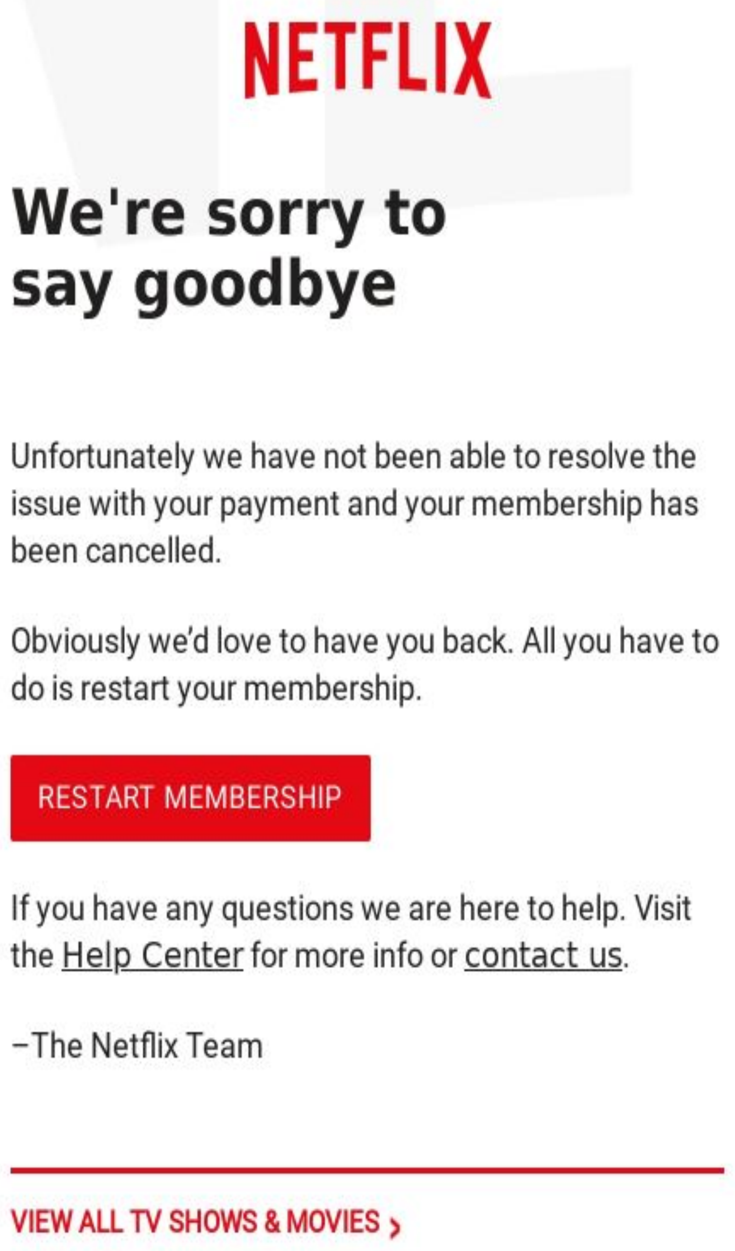
👈 *Yes, MFA is that "phone-thingy" we have to open grab a timed code for or that "USB-looking-thingy" we plug in.*

SOME EXTRA GOODIES

Tips for every IT team

3. TRAINING

- ✓ Subscribe to a service or company that sends out fake phishing emails. Do this often *(like weekly)*!
- ✓ Keep training sessions for users short and to point.
- ✓ Conduct training on Passwords: how to use Password Managers; how to not give away dumb information on Social Media, etc…



NETFLIX

We're sorry to say goodbye

Unfortunately we have not been able to resolve the issue with your payment and your membership has been cancelled.

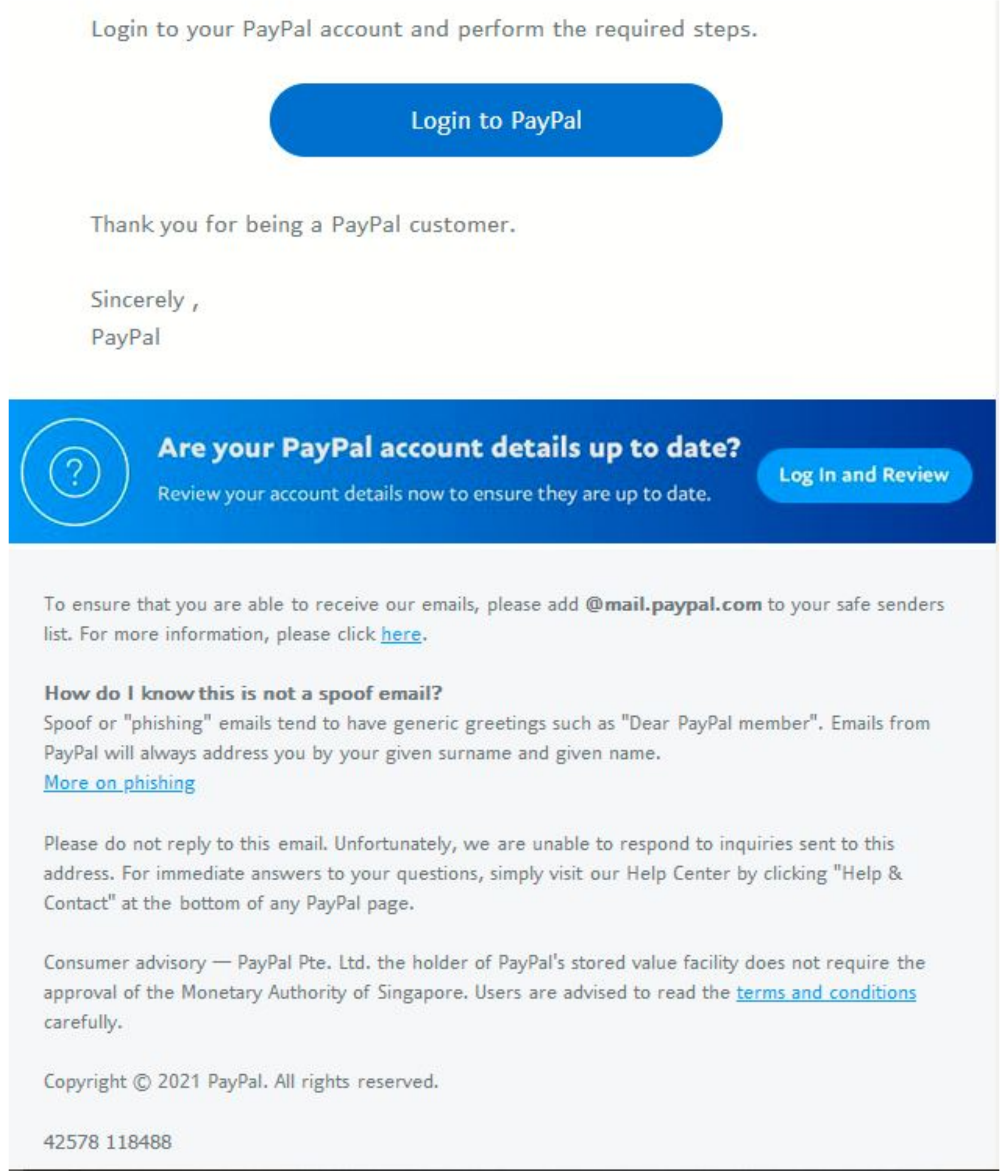
Obviously we'd love to have you back. All you have to do is restart your membership.

RESTART MEMBERSHIP

If you have any questions we are here to help. Visit the Help Center for more info or contact us.

–The Netflix Team

VIEW ALL TV SHOWS & MOVIES ›



Login to your PayPal account and perform the required steps.

Login to PayPal

Thank you for being a PayPal customer.

Sincerely ,
PayPal

Are your PayPal account details up to date?

Review your account details now to ensure they are up to date.

Log In and Review

To ensure that you are able to receive our emails, please add **@mail.paypal.com** to your safe senders list. For more information, please click here.

How do I know this is not a spoof email?
Spoof or "phishing" emails tend to have generic greetings such as "Dear PayPal member". Emails from PayPal will always address you by your given surname and given name.
More on phishing

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help & Contact" at the bottom of any PayPal page.

Consumer advisory — PayPal Pte. Ltd. the holder of PayPal's stored value facility does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

Copyright © 2021 PayPal. All rights reserved.

42578 118488

Appendix 8

SOME EXTRA GOODIES

Tips for every IT team

4. PAY FOR AN ASSESSMENT OR TESTING

- 💰 **Cybersecurity assessment**— Series of questions designed to help a business determine where they are vulnerable. A good one will not only interview IT, but also interview HR, Accounting, Vendor managers and C-level personnel *(CESO, CFO, CTO, etc.)*

- 💰💰 **Vulnerability assessment**— Designed to help a business determine where they are vulnerable. Trusted company deploys software or devices that search your network to point out vulnerabilities in your network. Highly technical!

- 💰💰💰 **Penetration testing**— Trusted company that basically ‘hacks’ into your network… highly technical.

- 💰💰💰💰 Others: **SOC 2, ISO 27001, DoD CMMC**— High-end, complicated, & most expensive

Appendix 9

SOME EXTRA GOODIES

Tips for every IT team

5. POWER OF 2'S

Use two people to verify large money transfers, wire transfers, etc.

Determine a dollar figure that you can't afford to lose as a business and require two people ALWAYS review it before payment is sent.

We see this constantly from Accountants, CFOs and CEOs and usually have to say "too bad, so sad.'

6. KILL RDP!!!

Remote Desktop Protocol— is a Microsoft-based remote access service that allows remote users to access services remotely.

If you're IT team uses RDP internally to manage servers, it should require MFA for every device they connect to.

Better yet, help your IT team get rid of it once and for all, and then replace it with an SSL based VPN.

Note: Hackers LOVE RDP.... so take it out back to the woodpile and give it a trouncing

7. PASSWORD MANAGERS

Learn how to use them!

Teach a class to all users on how to use them properly & consistently

Use them at home as well!

A few quality examples:
LastPass, BitWarden, DashLane..

And some browser-based examples:
Chrome, Firefox, Opera

Also these Password Repositories:
KeePass, KeePassium, Strongbox