Project Management Institute New Jersey

Implementing an Information Security Management System (ISMS)

November 17, 2020

Manny Kahn
info@ismllc.com | Manny.k.347@gmail.com
1 (732) 763-2472
https://www.ismllc.com
https://www.linkedin.com/in/khanmanny
https://www.linkedin.com/company/information-security-management-llc


Cybersecurity

Agenda

GENERAL

- Who am I?
- Quick Polls
- Size in $$$
- Certifications
- What do I need to know about Cybersecurity?
- Organizational Structure & Organizational Wide Wins
- Roadmap = Slate: What's Next?

SECURITY OPERATIONS

- Incident Response
- Security Operations

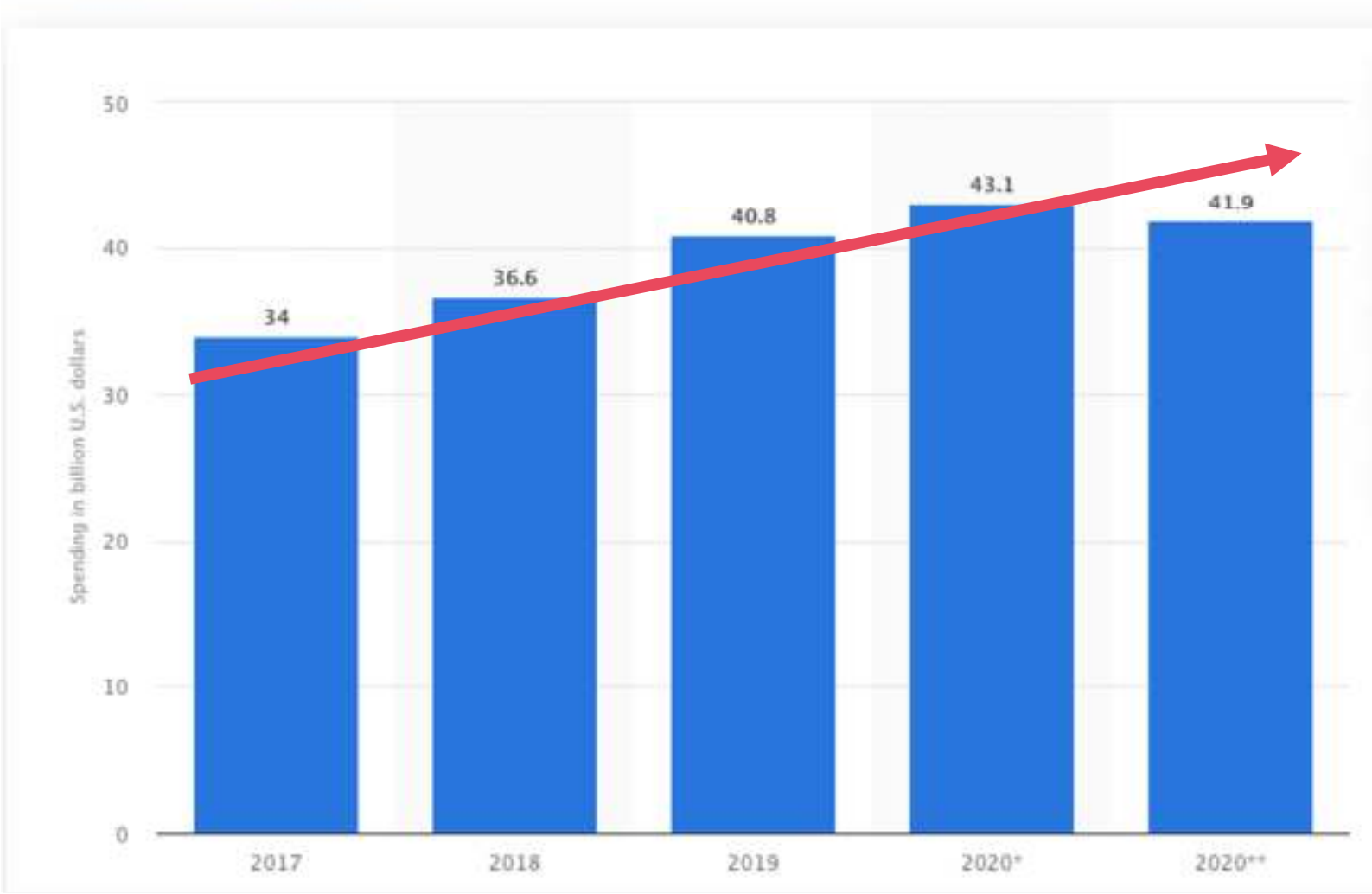
PHISHING

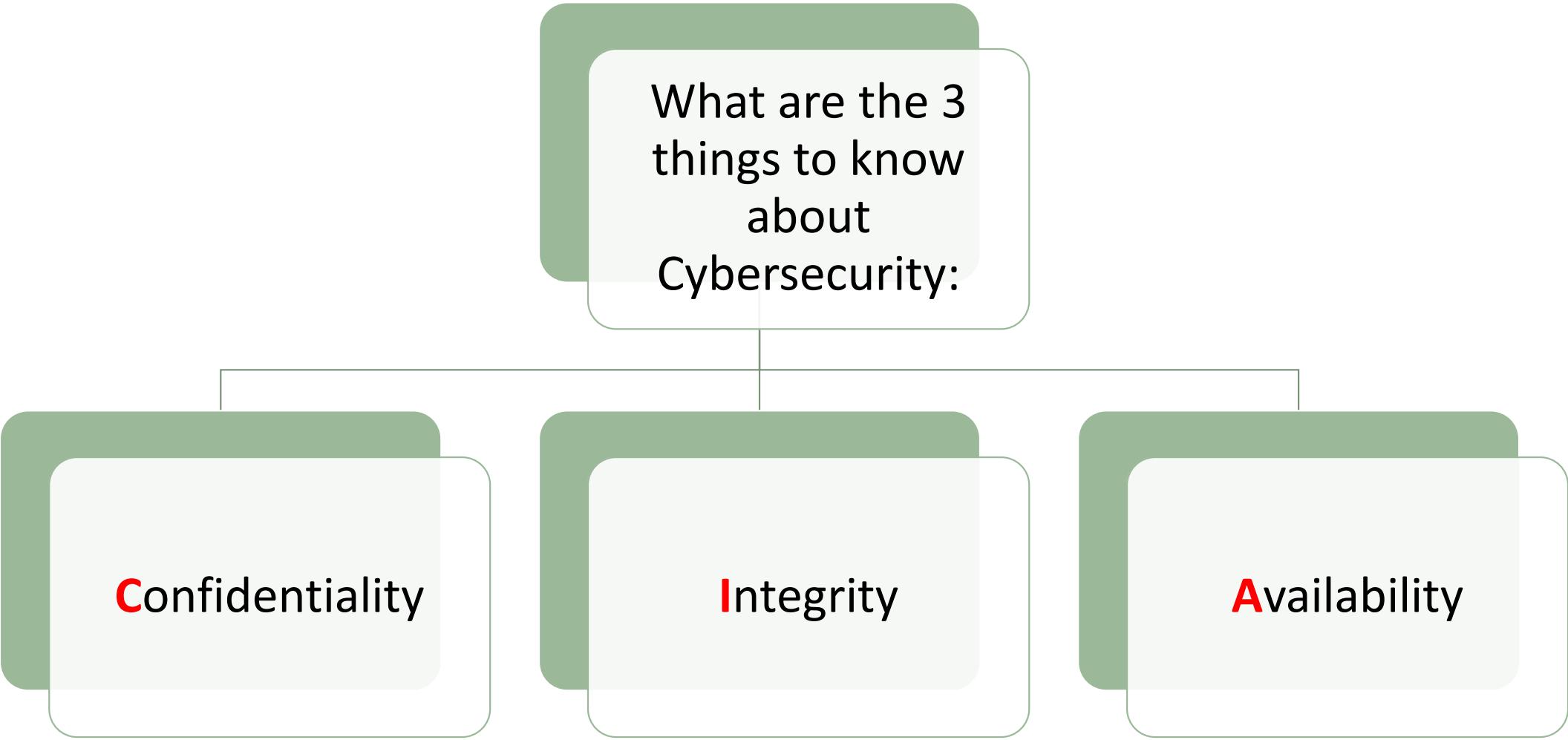
- Example Phishing E-mail
- Training the User

OPEN DISCUSSION

Spending on cybersecurity worldwide from 2017 to 2020

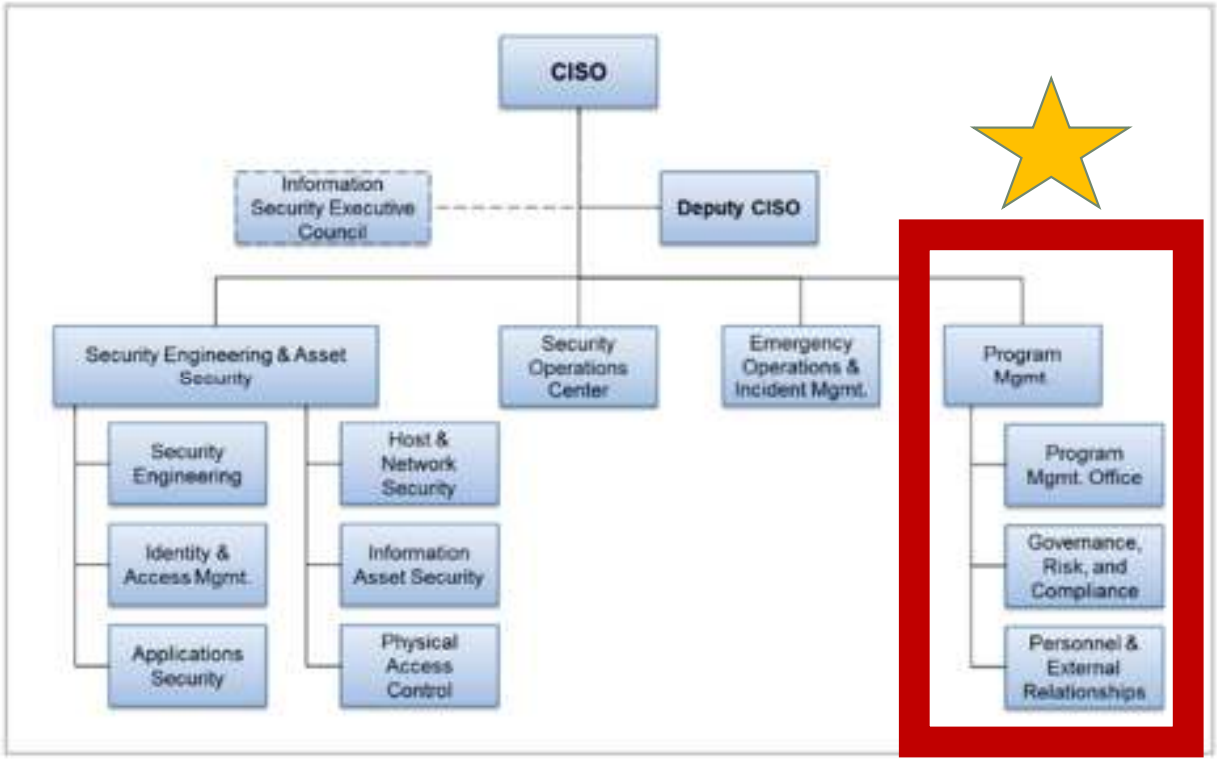
(in billion U.S. dollars)




What are the 3 things to know about Cybersecurity:
Confidentiality
Integrity
Availability

Organizational Structure

Ideal security organization based on research by Carnegie Mellon University that can be found here



Cybersecurity Certifications

ISACA	(ISC)²	AWS
CISM	CISSP	AWS Certified Security - Specialty
CISA	CCSP	

Organization-Wide

- **Ensure cross training of your Cybersecurity team on your security owned tools and solutions at a basic level.**
- **Make Cybersecurity Operations (Incident Response) your centerpiece when starting out with your Cybersecurity program.**
- **Build relationships and ask your Technology Teams why the technical standards are the standards.**
- **Test & train your users often and thoroughly for their awareness of Cybersecurity best practices.**

Roadmap = Slate: What's Next?

1. **Antivirus:** Deploy and establish a single endpoint protection agent on both servers and workstations.

2. **Virtual Private Network:** Deploy an Always On VPN solution whenever any user is connecting to your network.

3. **Information Technology Service Management (ITSM) Tool:** All incidents, requests, and/or tasks should be raised through an ITSM tool for action and resolution.

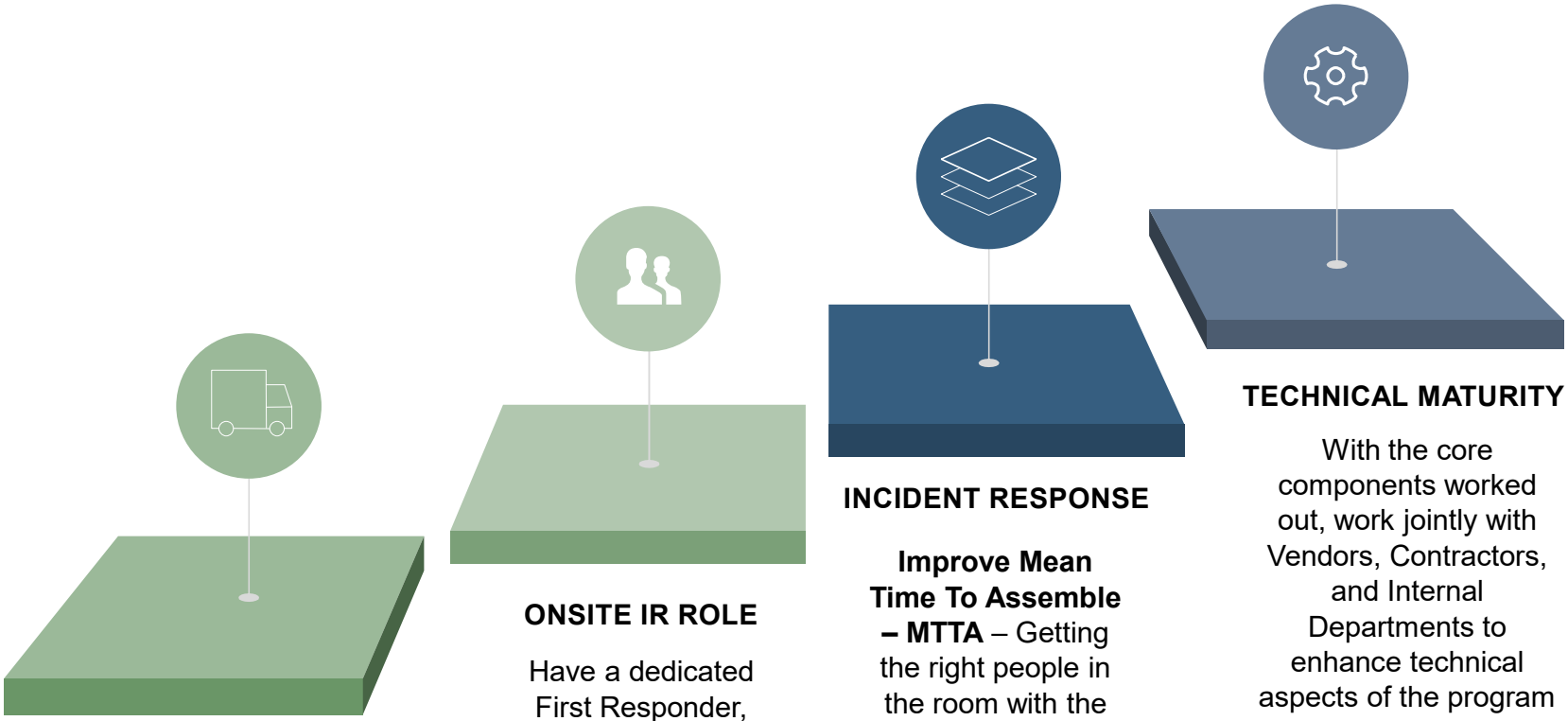
4. **Vulnerability Management:** Use a vulnerability management tool to identity vulnerabilities, score them, and apply the fixes all through the same console.

5. **SIEM & SOAR:** Buy and implement a Security Information and Event Management followed by a Security Orchestration, Automation, and Response.

Security Operations

INCIDENT RESPONSE

Security Operations



STARTING THE PROCESS

Are images being built with security in mind?

ONSITE IR ROLE

Have a dedicated First Responder, improved speed, and enhanced customer experience

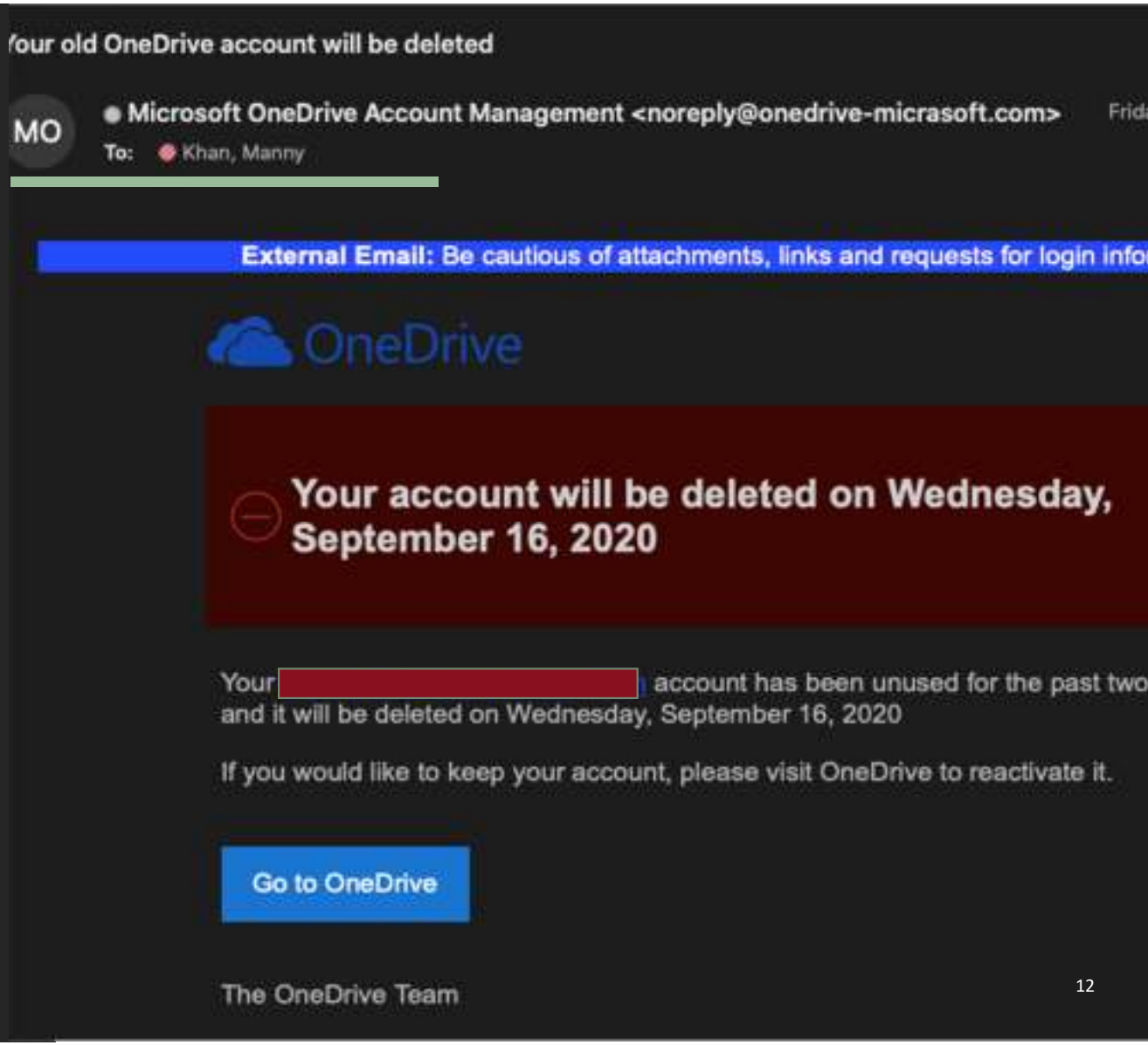
INCIDENT RESPONSE

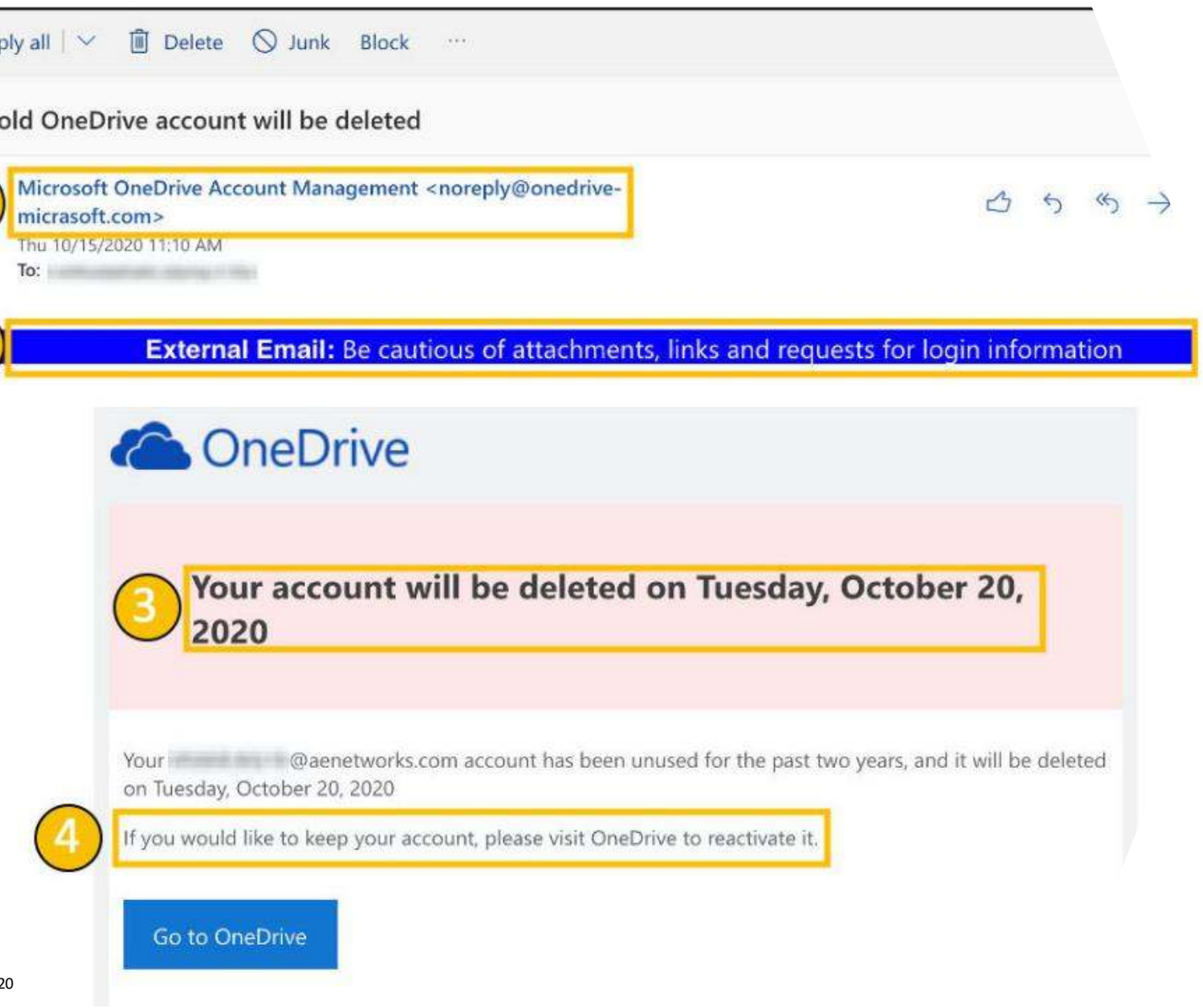
Improve Mean Time To Assemble – MTTA – Getting the right people in the room with the right tools to address the problem.

TECHNICAL MATURITY

With the core components worked out, work jointly with Vendors, Contractors, and Internal Departments to enhance technical aspects of the program to support new Processes, SOPs, and expectations.

Phishing Simulation – How to Spot & What to do





Let's Review Together

20

- INFO@ISMLLC.COM | MANNY.K.347@GMAIL.COM
- +1 (732) 763-2472
- HTTPS://WWW.LINKEDIN.COM/IN/KHANMANNY/
- HTTPS://WWW.LINKEDIN.COM/COMPANY/INFORMATION-SECURITY-MANAGEMENT-LLC
- HTTPS://WWW.ISMLLC.COM/