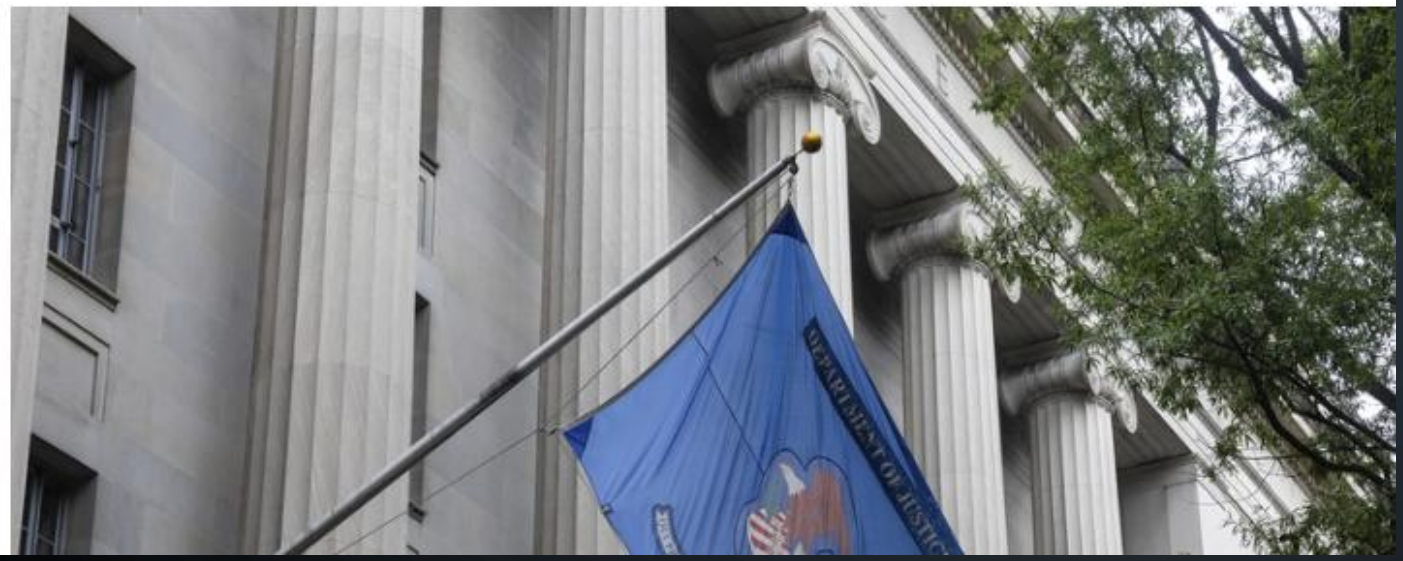
From the Field
Cybersecurity in 2026

Federal court filing system hit in sweeping hack

The identities of confidential court informants are feared compromised in a series breaches across multiple U.S. states.



tack knocks Alaska courts

system deactivated nearly all its external IT syst
t servers," though cases are still proceeding.

MAY 5, 2021

CYBERSECURITY

October cyberattack exposed data Kansas court investigation finds

An investigation by the Kansas Office of Judicial Administration year may have exposed personal information of 150,000 people.

BY SOPHIA FOX-SOWELL • MAY 7, 2024

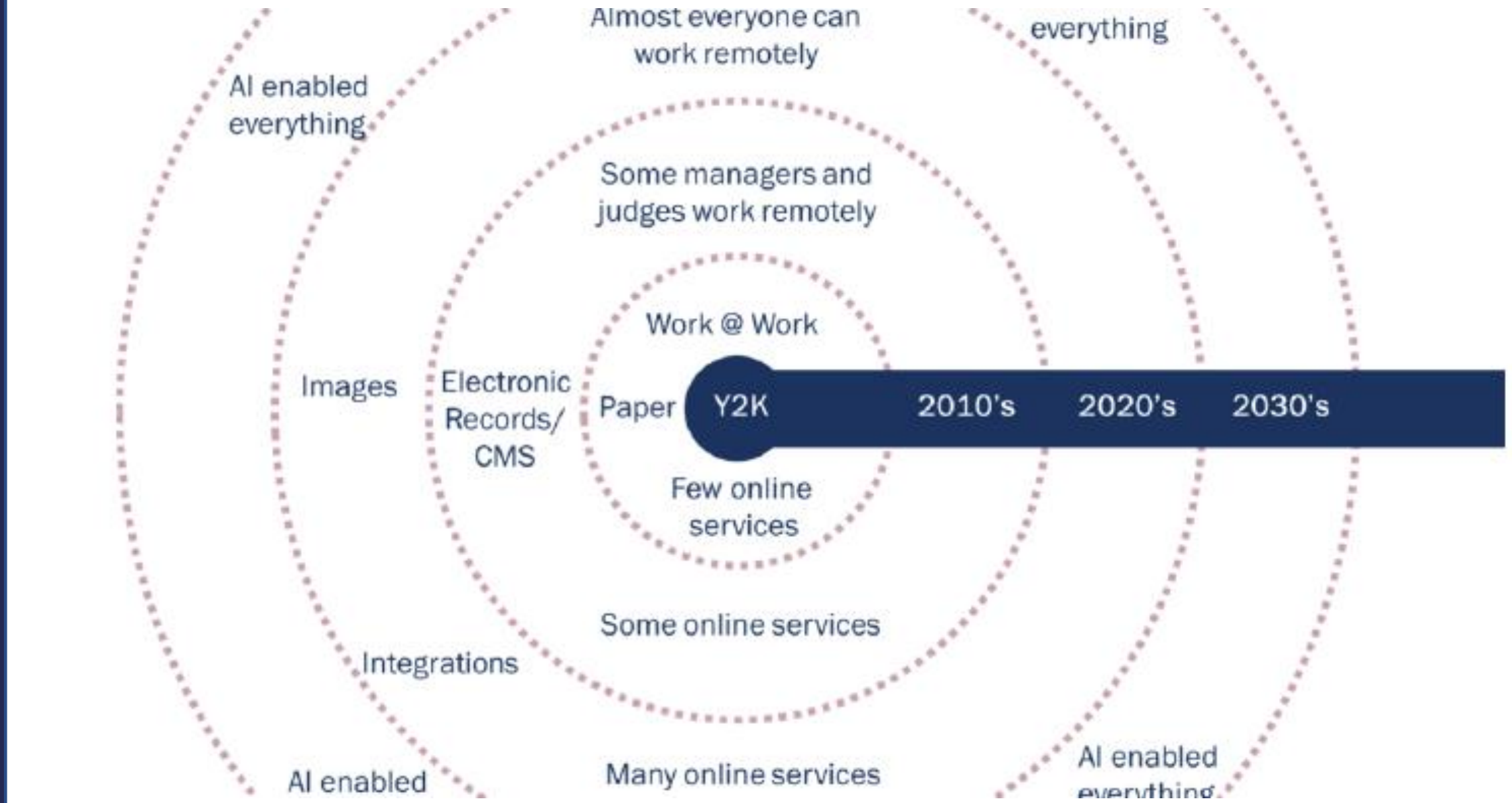
DDoS attack on Pennsylvar system knocks out filing sy payment site

Technology

Georgia court system struck by ransomware attack

July 2, 2019 / 9:50 AM EDT / CBS News

Add CBS News on Google


Almost everyone can work remotely
everything
AI enabled everything
Some managers and judges work remotely
Work @ Work
Images
Electronic Records/ CMS
Paper
Y2K
2010's
2020's
2030's
Few online services
Some online services
Integrations
AI enabled
Many online services
AI enabled

DECADE OF CHANGE

BE IT FURTHERED RESOLVED, that the Conference of Chief Justices and Conference of State Court Administrators urge the National Center for State Courts (NCSC) to enhance the cybersecurity consulting and technical assistance services offered by NCSC to assist state courts in their efforts to improve cybersecurity.

Adopted as proposed by COSCA/NACM Joint Technology Committee at the COSCA 2021 Midyear Meeting and by the CCJ Board of Directors on December 22, 2021.

NCSC Workshops

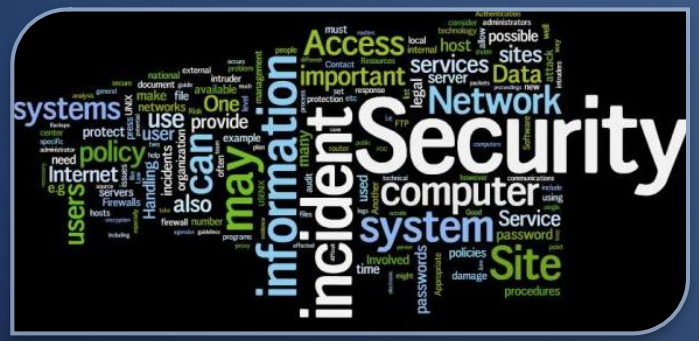
Strengthening your court's response to a cyberattack

GUIDING DOCUMENTS

Cybersecurity Basics for Courts

Cybersecurity Incident Planning and Response for Courts

TOPICS FOR TODAY



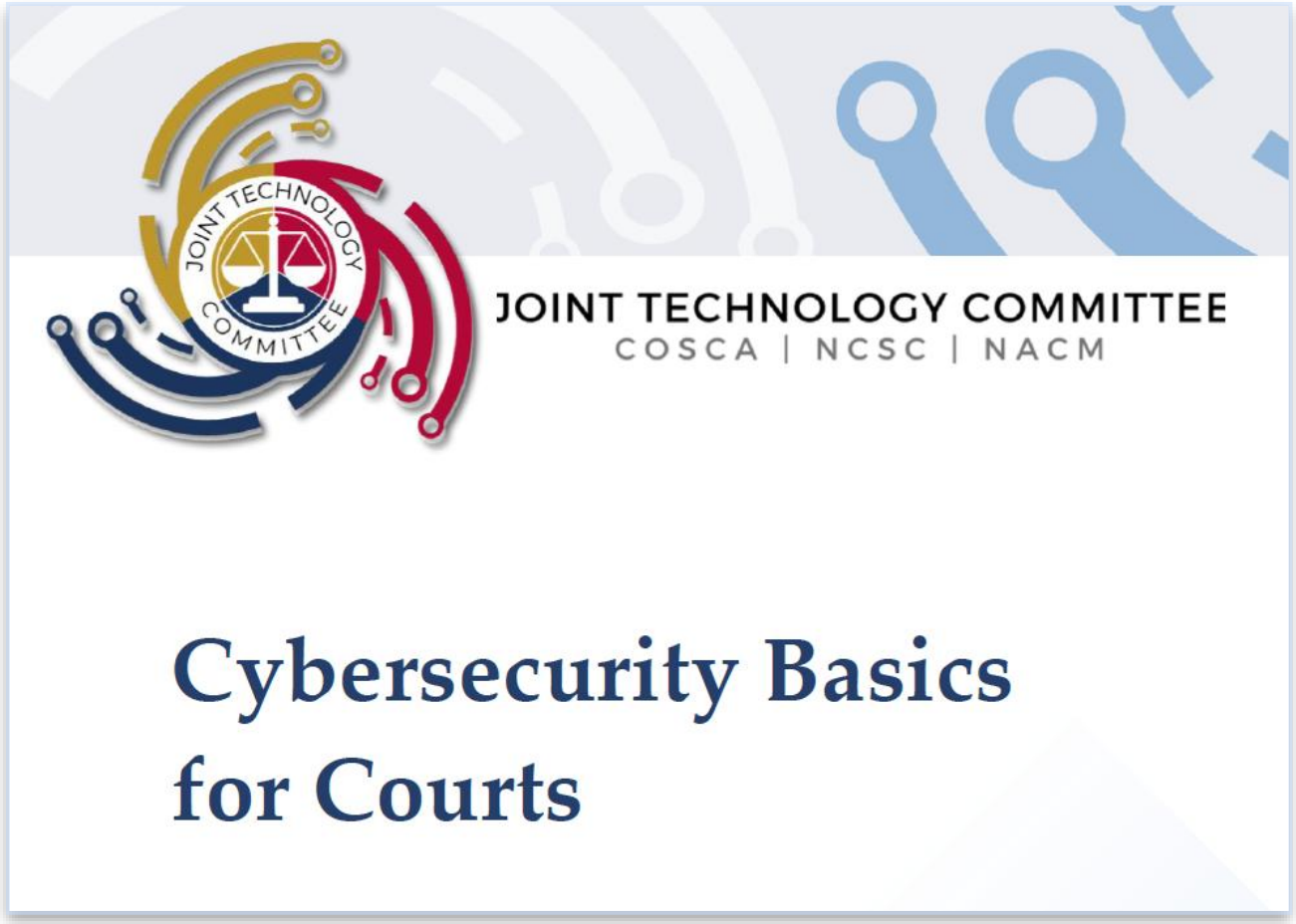
CYBERSECURITY BASICS

CASE STUDY EXAMPLES

PLANNING FOR RECOVERY

ADDITIONAL SESSIONS

- Group Discussions
- Tabletop Exercise
- Resources



CYBERSECURITY PRINCIPLES APPLIED TO COURTS AND TRANSLATED INTO HOW WE DO BUSINESS

EXECUTIVE SUMMARY

CYBERSECURITY IS NO LONGER AN OPTIONAL CONCERN, IT IS CRITICAL OPERATIONAL IMPERATIVE

UNDERSTAND COMMON THREATS AND OPPORTUNITIES

INDUSTRY BEST PRACTICES

BUILD STRONGER, MORE SECURE DIGITAL ENVIRONMENT THAT SUPPORTS JUSTICE AND SERVICE DELIVERY

Cybersecurity by the Numbers: 2025 Snapshot

Average time to identify and contain a breach (breach lifecycle)	Average cost of a data breach		
	Global	US	Healthcare Sector
241 days	$4.44M	$10.22M	$7.42M (highest of any sector)

Most common initial attack vector	Malicious or criminal attack
Phishing (16%)	51%

Average cost savings with a cybersecurity incident response team and testing
$1.49M[6]

WHY CYBERSECURITY MATTERS FOR COURTS

- Courts are prime targets
- Threats are constant
- Disruption has serious consequences
- Preparation is key
- Everyone plays a role


95%
of all successful cyber attacks
is caused by human error
Source: IBM Cyber Security Intelligence Index

CYBERATTACK

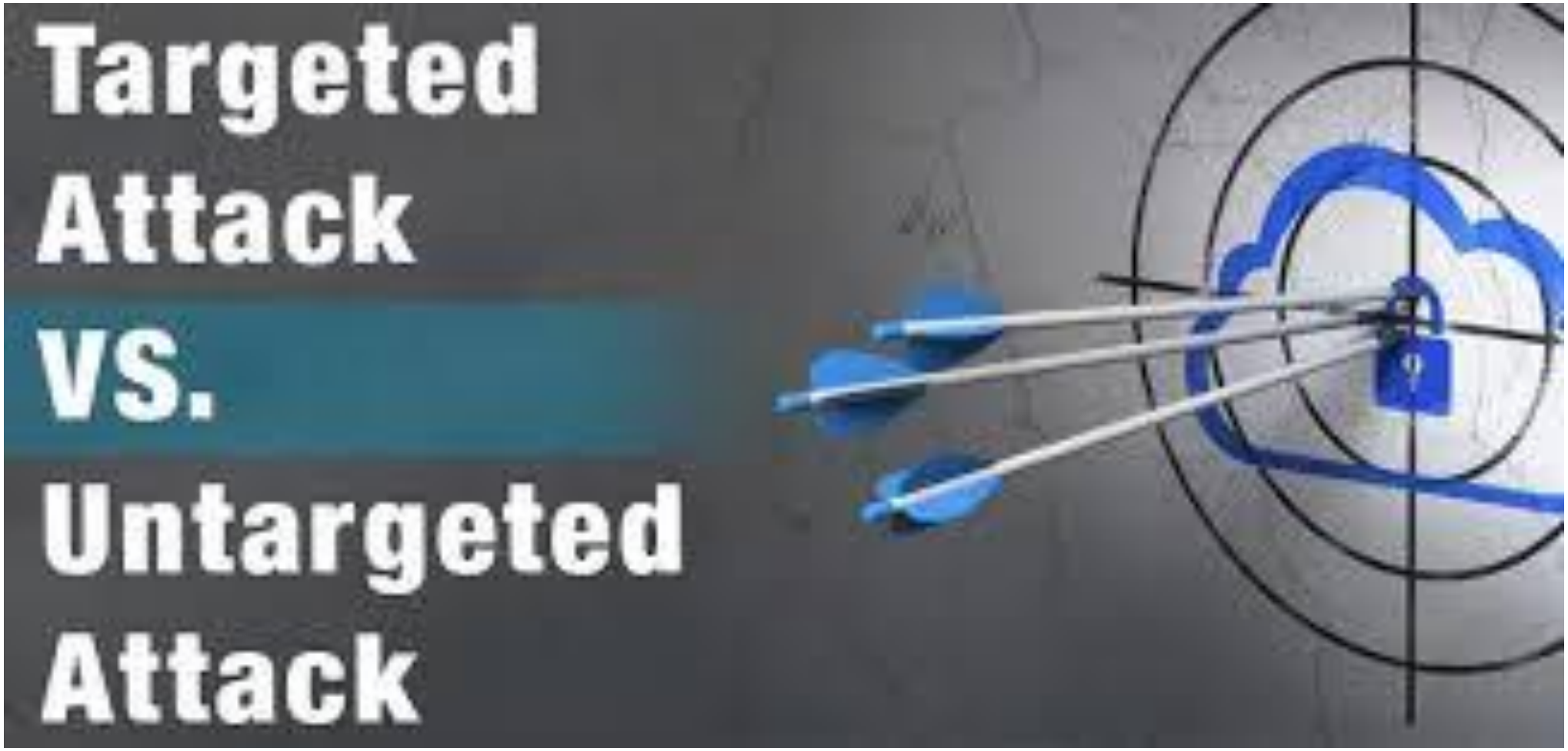
(1) Deliberate attempt by bad actor

(a) disrupt services

(b) gain unauthorized access

COMMON TYPES OF ATTACKS

- Malware and viruses
- Denial of Service (DOS) or distributed denials of services (DDOS)
- Zero-day exploits
- Ransomware
- Unauthorized access


Targeted
Attack
VS.
Untargeted
Attack


CONVENIENCE
VS SECURITY

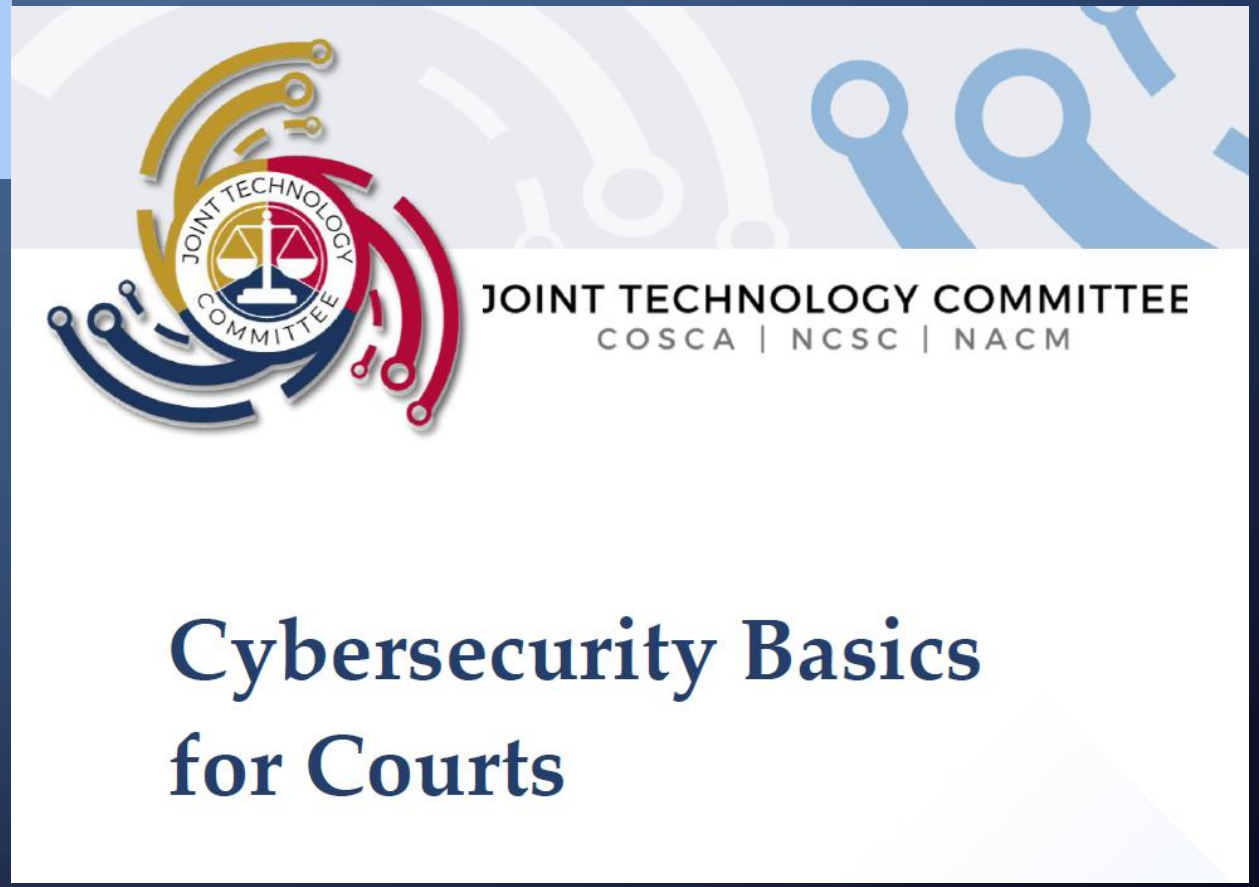
Notable Recent Cyberattacks on U.S. State Courts

- **Los Angeles County Superior Court (July 19, 2024)**
  A ransomware attack forced the closure of all 36 courthouses, the largest unified trial court in the U.S., on a Monday following detection on Friday. Systems from jury portals to case management were disabled. The court restored basic functionality by Tuesday and full service within about eleven days. There was no evidence that user data had been compromised.[7]
- **Cleveland Municipal Court, Ohio (February–March 2025)**
  On February 23, 2025, the court suspended all internal systems in response to a suspected ransomware incident.[8] The Ohio National Guard's Cyber Reserve Force assisted in the investigation. The Qilin ransomware group later claimed responsibility. Most operations, including online services and hearings, were suspended until reopening on March 12, 2025.[9]

APPENDIX A
ABOUT CYBERATTACKS

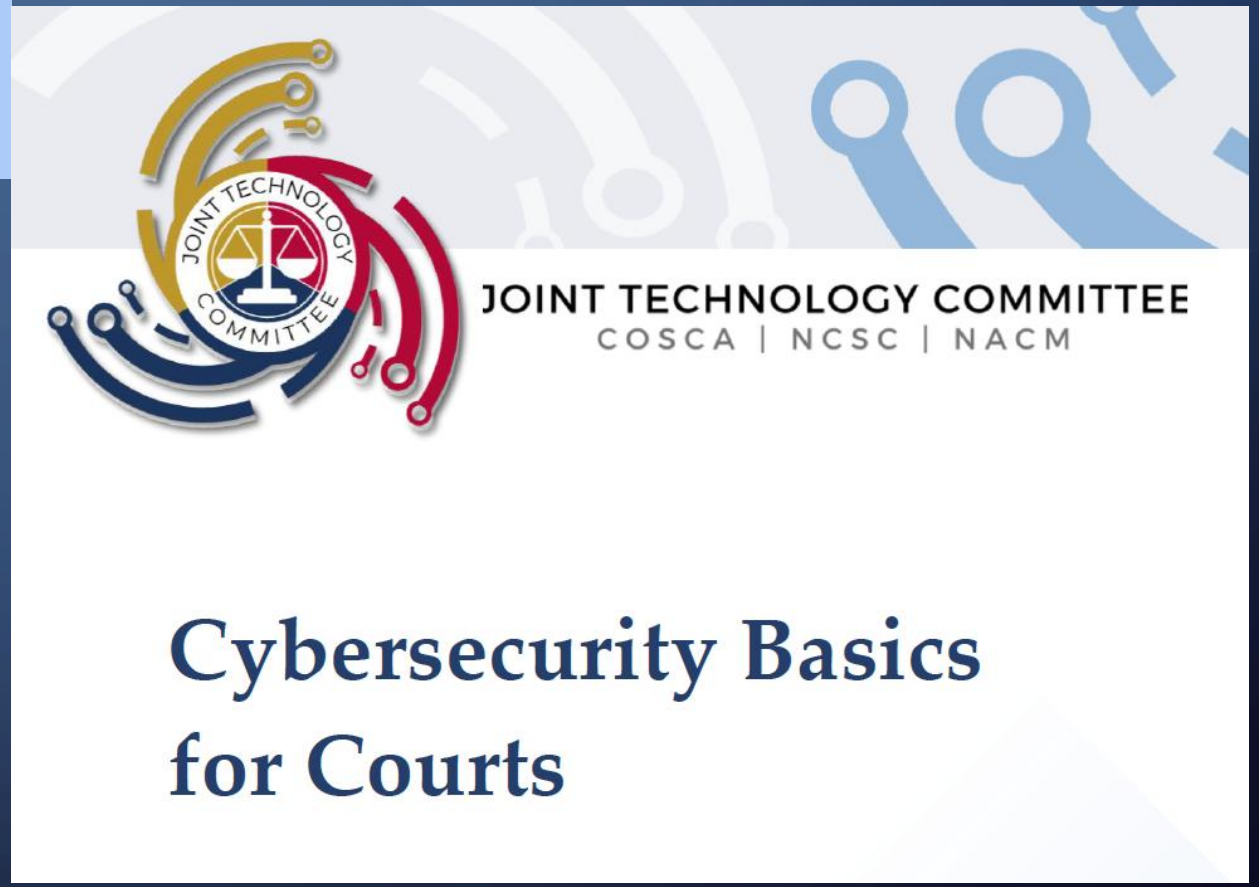
Useful technical details about Cyberattacks

6 pages with basic definitions for non-technical audience



APPENDIX B
CYBERSECURITY DISCUSSION GUIDE

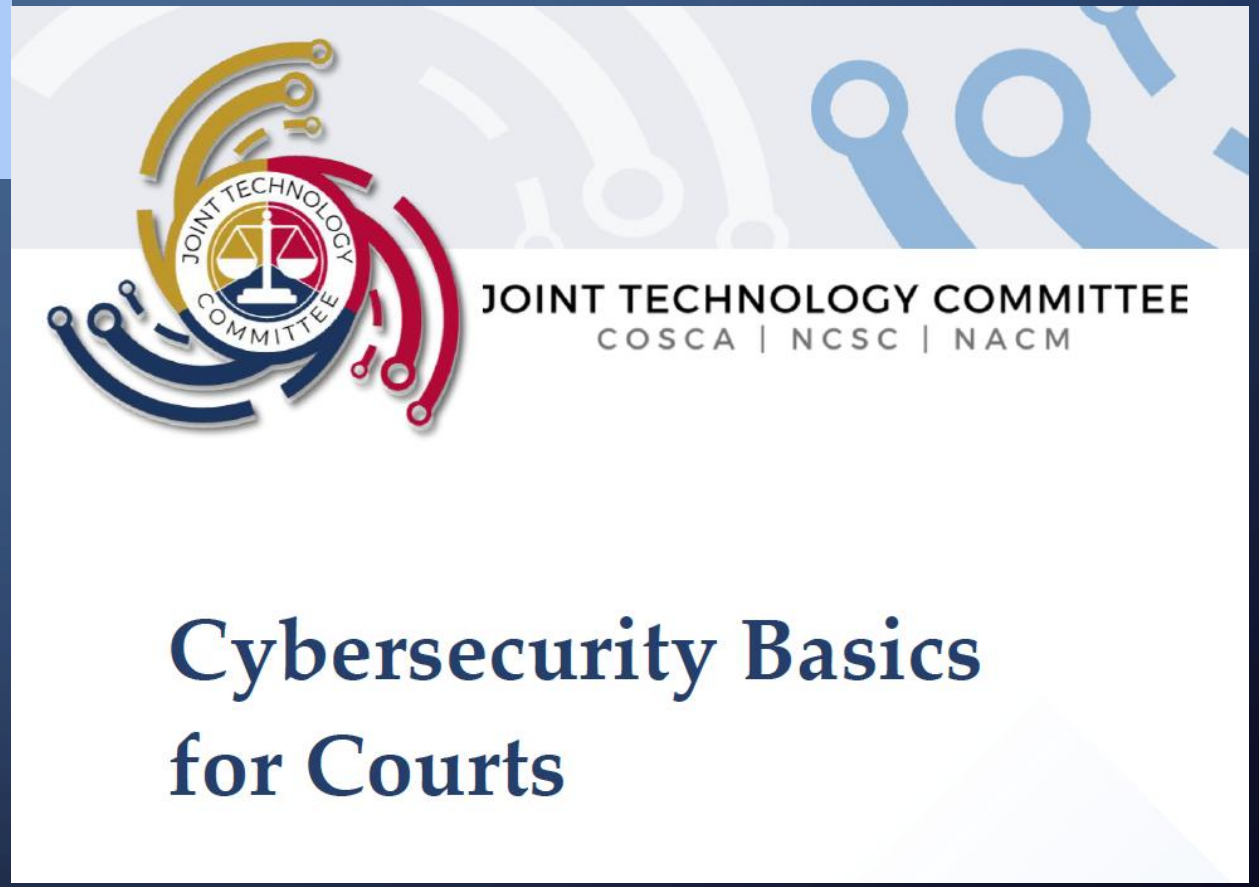
List of questions to facilitate conversations between administration and technical teams, including county, vendor and IT staff



APPENDIX C
TAKING ACTION

Useful checklist on next steps

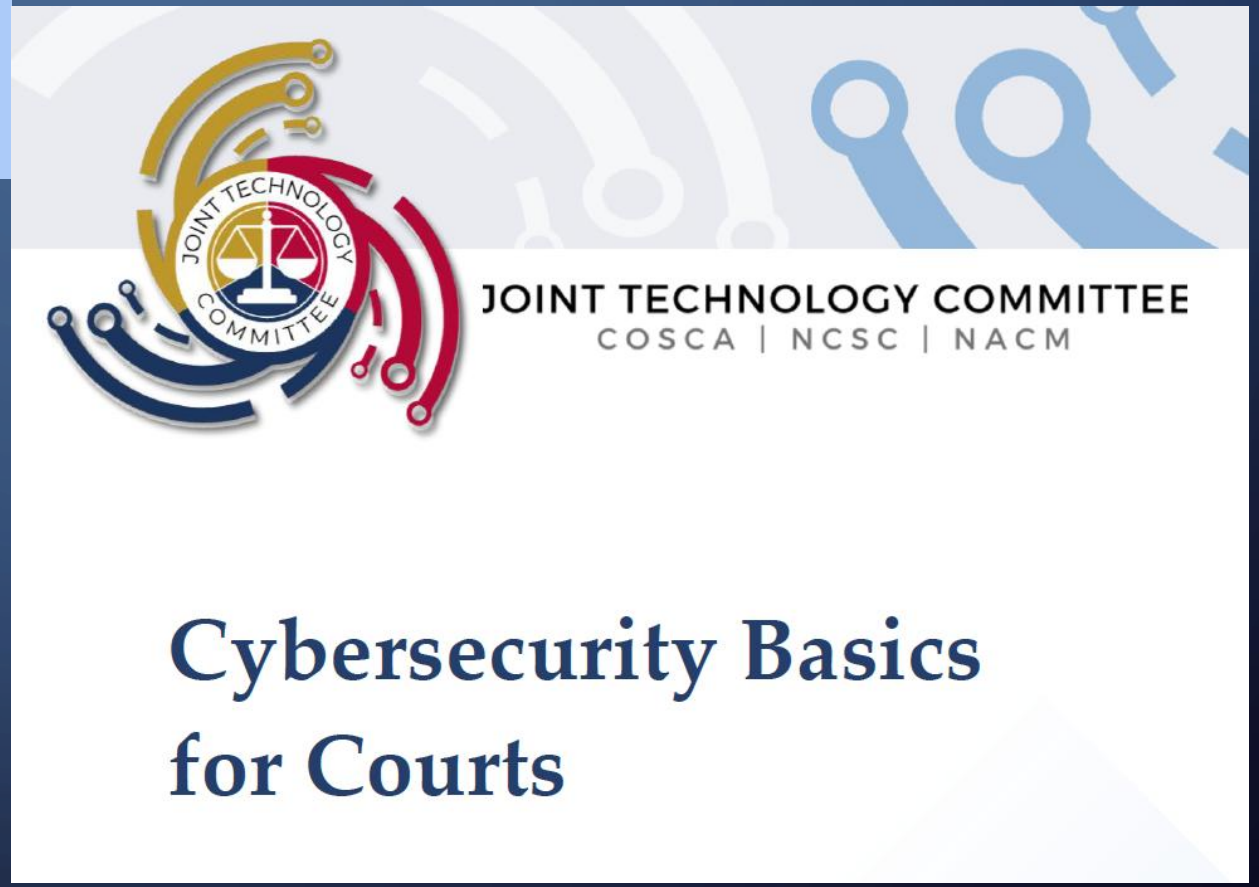
Depending on your court and technology structure some items may or may not apply



APPENDIX D
CYBERSECURITY GOVERNANCE CHECKLIST FOR COURTS

15-point checklist to guide technical understanding for COOP planning

Depending on your court and technology structure some items may or may not apply



PREVENTION AND PREPARATION

HUMAN FIREWALL

Own it

Talk about it

Court Champion

Resources

INVESTMENT

Time and Money

Court and partners

Planning time

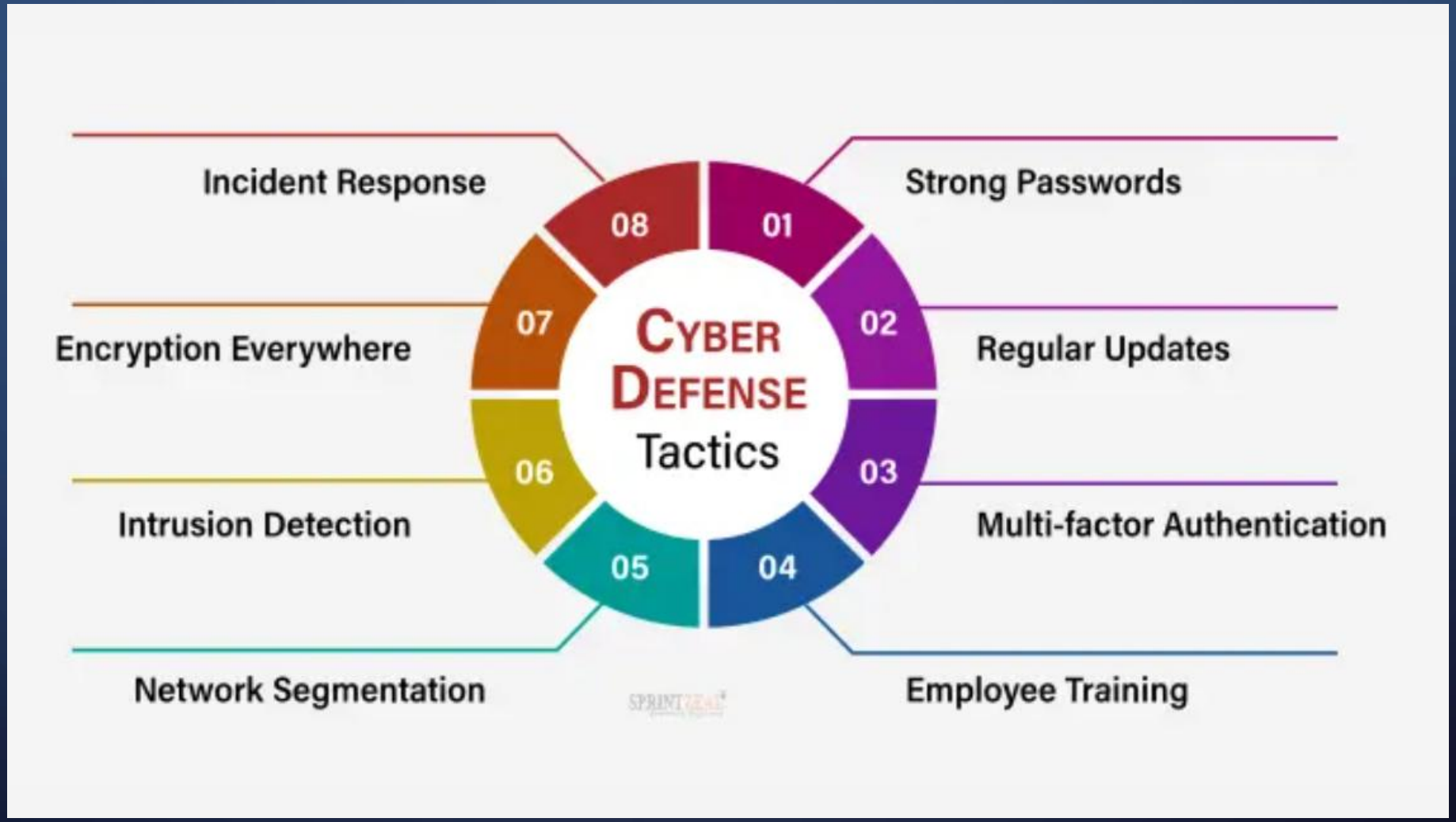
INCIDENT RESPONSE

Where to start?

Incident response

Investigation

Recovery

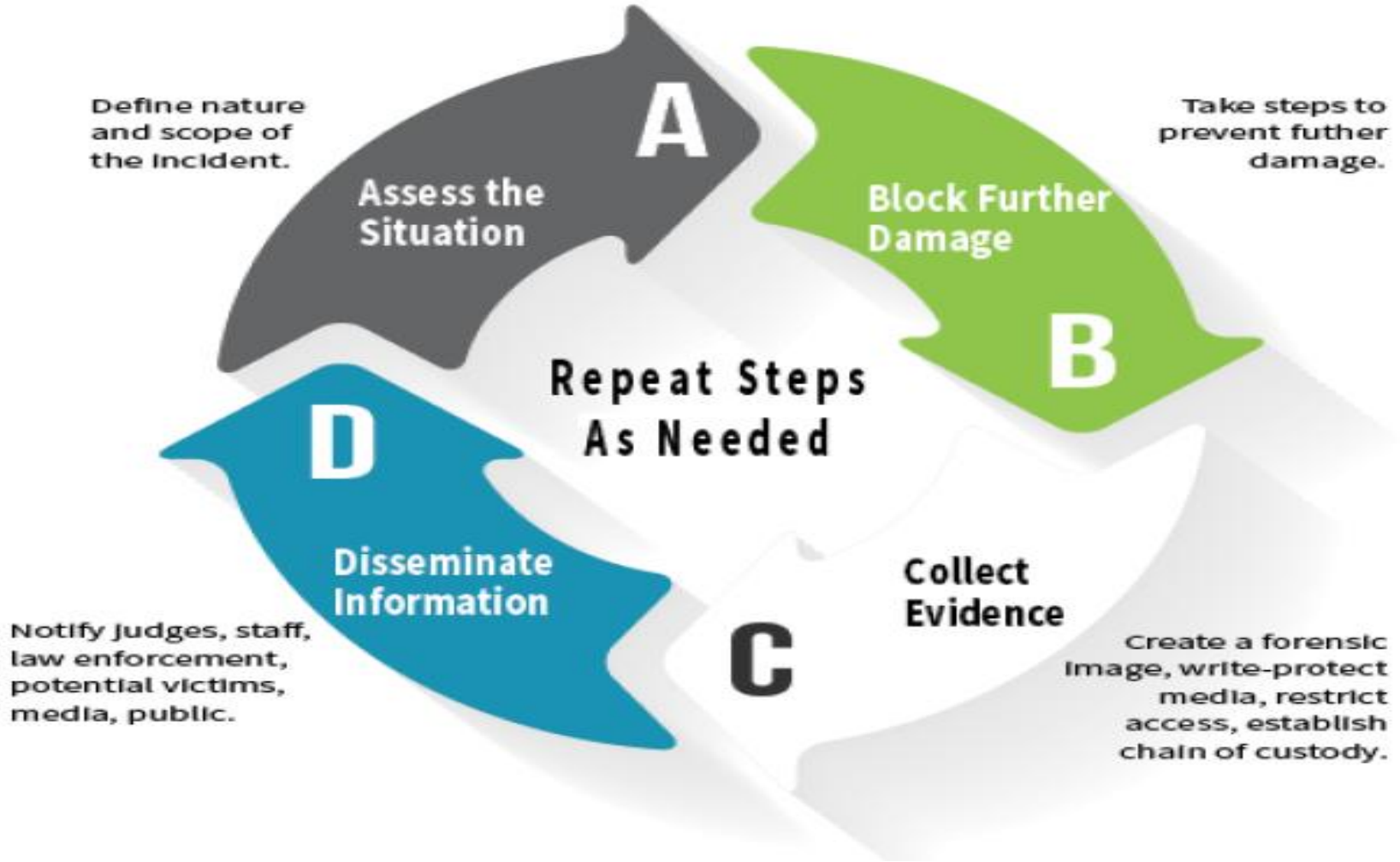

Incident Response
08
01
Strong Passwords
Encryption Everywhere
07
Cyber
Defense
Tactics
02
Regular Updates
06
03
Intrusion Detection
Multi-factor Authentication
05
04
Network Segmentation
Employee Training

JOINT TECHNOLOGY COMMITTEE

COSCA | NCSC | NACM

Cybersecurity Incident Planning and Response for Courts

CYBER INCIDENT RESPONSE



PLANNING FOR THE INEVITABLE

- Outages
- System dependencies

TIME TO RECOVERY

It depends…

Scope

Impact

Encrypted or exfiltrated data / files

Resource focus – Investigation vs restoration

BIGGEST CHALLENGES – SERVICE ORGANIZATION

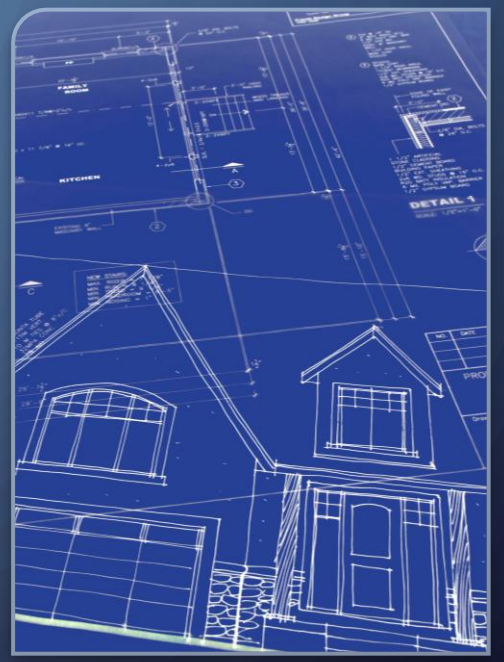
Used to expediency and relationships

Give technical teams time to work and understand

Scope and impact drives response and timelines

LAYING A STRONG FOUNDATION

An effective incident response plan requires that several key components be in place before an incident occurs

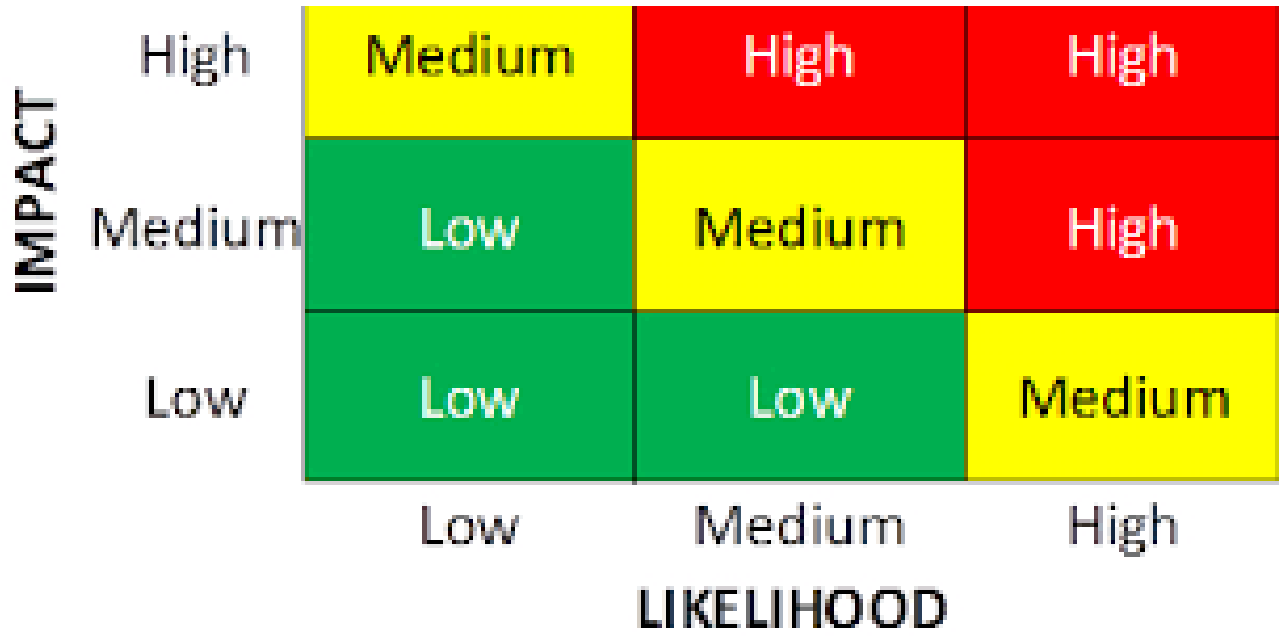


IDENTIFY DATA ASSETS

- Build an inventory
- Account for third party vendor or county assets
- Understand where Court responsibilities start and end

Workbook: End Point Inventory Tool

RISK ASSESSMENT AND ANALYSIS



Likelihood vs impact

Acceptable downtime - **Recovery Time Objective**

Acceptable data loss – **Recovery Point Objective**

Workbook: Technology Priorities

DATA BREACH AND NOTIFICATION

UNDERSTAND AND HAVE A WRITTEN POLICY

Workbook: Essential Functions table

VENDOR / THIRD PARTY MANAGEMENT

- What systems and services are vendor dependent?
- Which systems and services are county or state dependent?
- Understand what happens if those systems have outages beyond the scope of the court.
- Understand Service Level Agreements (SLA) and contract terms – notifications, recovery, updates, incident response timelines

Workbook Critical IT Vendors

DEVELOP A PLAN

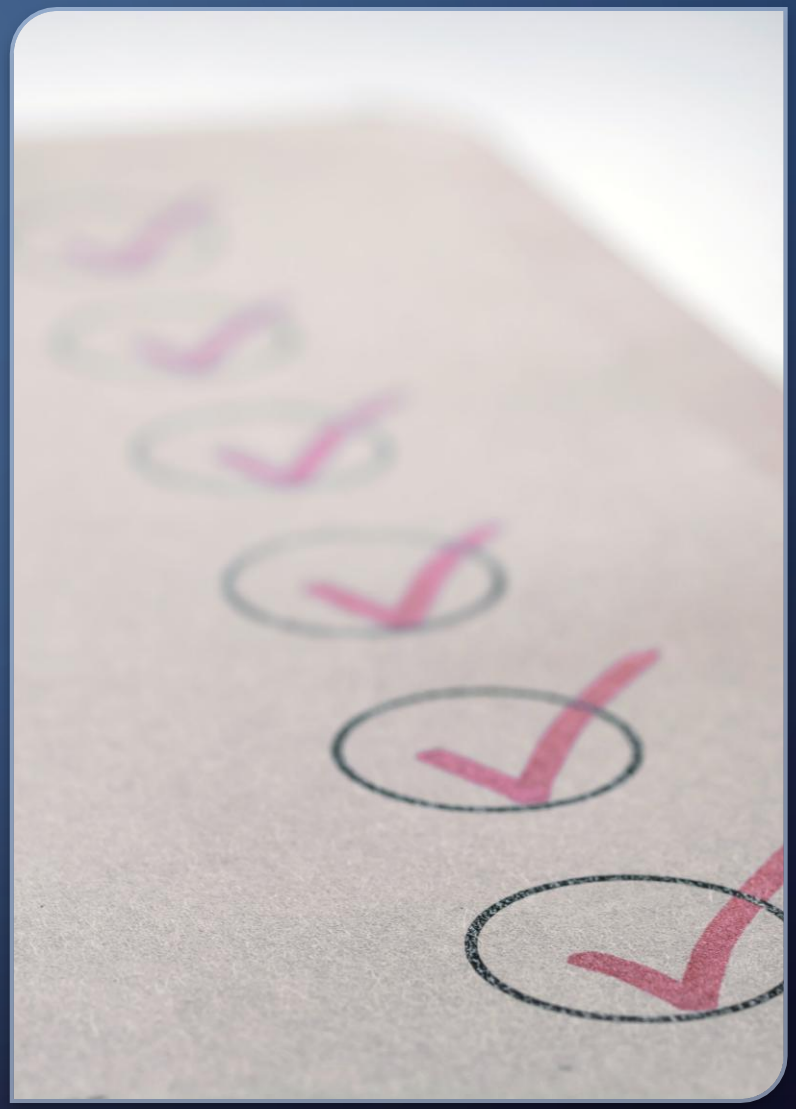
Who will be involved?

What roles for each individual

How to communicate – internal and external

What steps is each person responsible for?

When must each task be completed?



Workbook Crisis Management Team

COMMUNICATION PLAN

Create preapproved draft communications

- Designated spokesperson
- Court staff
- Third party

Workbook Communication Modalities

FORENSICS VS RECOVERY

Law enforcement reports

Insurance

Incident response support

Communication services

Critical operations

Electronic filing & documents

Payment portals

Infrastructure services

CYBERSECURITY TABLETOP EXERCISES

- Test and update plan regularly
- Phishing simulations – staff training
- Cybersecurity training – technical staff

APPENDIX B
CYBERSECURITY TABLETOP EXERCISES

Practice Scenario Exercise

Wendy Hosch
Assistant Director of Information Technology
Administrative Office of Pennsylvania Courts
Wendy.hosch@pacourts.us

Tyler Simmons
Cybersecurity Officer
Administrative Office of Pennsylvania Courts
Tyler.Simmons@pacourts.us