

Privacy Cyberwarfare

DR. LISA MCKEE

SEPTEMBER 20, 2023



Dr. Lisa McKee

NIST

PROUD MEMBER OF
Accredited Standards Committee X9[™]
Inc.
Financial Industry Standards

women in
CYBERSECURITY
WiCyS

RSA[®]Conference



UAH
THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

UCCS
University of Colorado
Colorado Springs

DS
DAKOTA STATE
UNIVERSITY

ONE IN TECH[™]

An ISACA Foundation



Privacy Cyberwarfare

As nation-state actors grow their information warfare capabilities, individuals suffer as part of coordinated and targeted attacks on organizations. Threat actors are weaponizing data causing life threatening harms. This session presents a new privacy cyberwarfare framework for privacy-related harms—tactics, techniques and mitigation strategies to address sophisticated privacy threat actors.

After completing this session, participants will be able to:

- Define privacy cyberwarfare.
- Understand how to monitor and protect against cyberwarfare to prevent security incidents.
- Take away tips on using the MITRE ATT&CK Framework to combat privacy cyberwarfare and protect against privacy harms.
- Observe techniques for reporting and negotiating with leadership and the board on cyberwarfare challenges and changes.

Learning Objectives

What is Privacy Cyberwarfare?

Monitor and Protect Against Privacy Cyberwarfare

Utilizing the MITRE ATT&CK Framework

Techniques for Reporting and Negotiating with Leadership

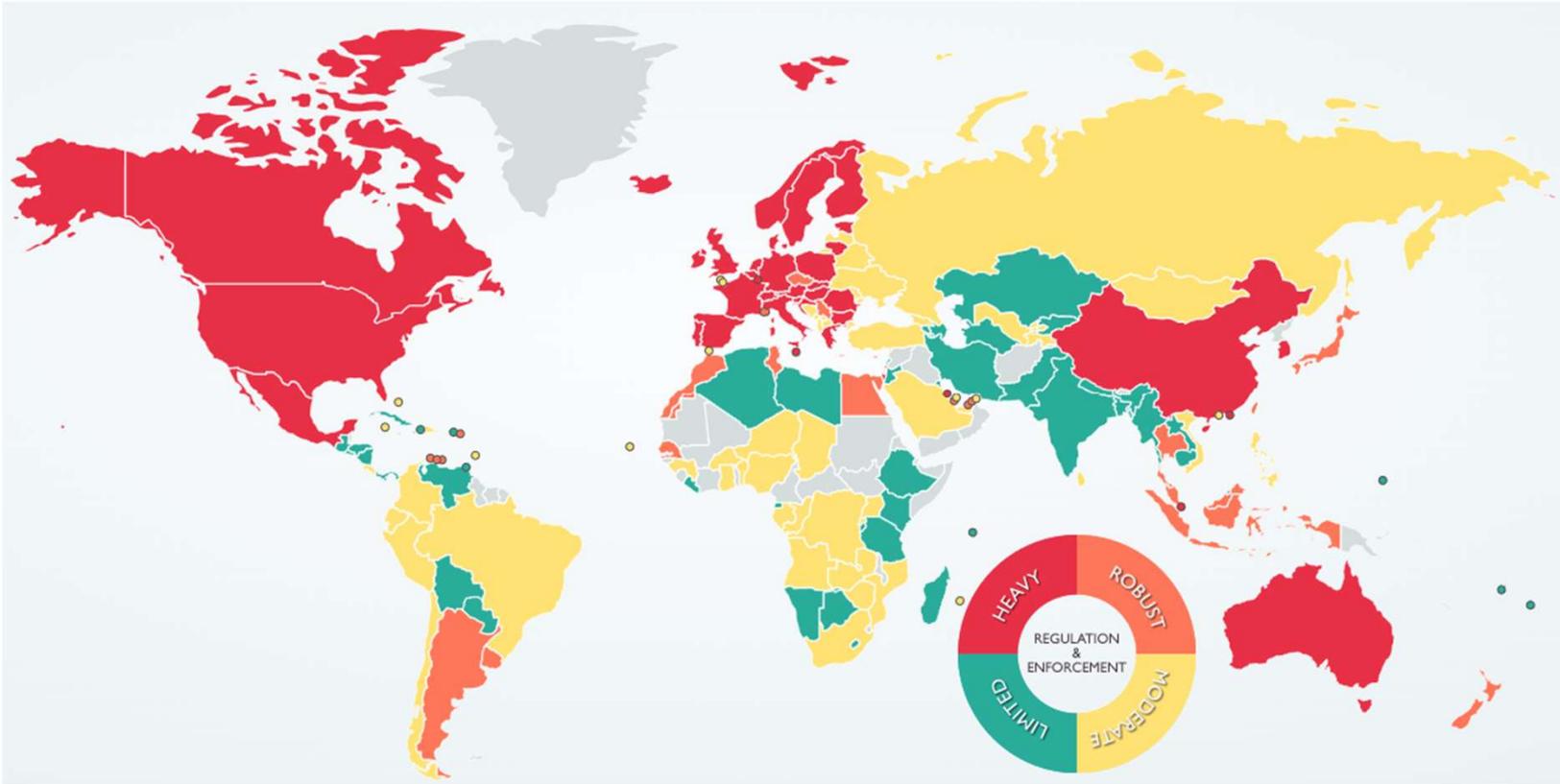
Privacy Landscape

FIPPs Privacy Principles

- 1. Access and Amendment.** Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.
- 2. Accountability.** Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors and should provide appropriate training to all employees and contractors who have access to PII.
- 3. Authority.** Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.
- 4. Minimization.** Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.
- 5. Quality and Integrity.** Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
- 6. Individual Participation.** Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.
- 7. Purpose Specification and Use Limitation.** Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
- 8. Security.** Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
- 9. Transparency.** Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.



DLA Piper - Global Privacy Laws



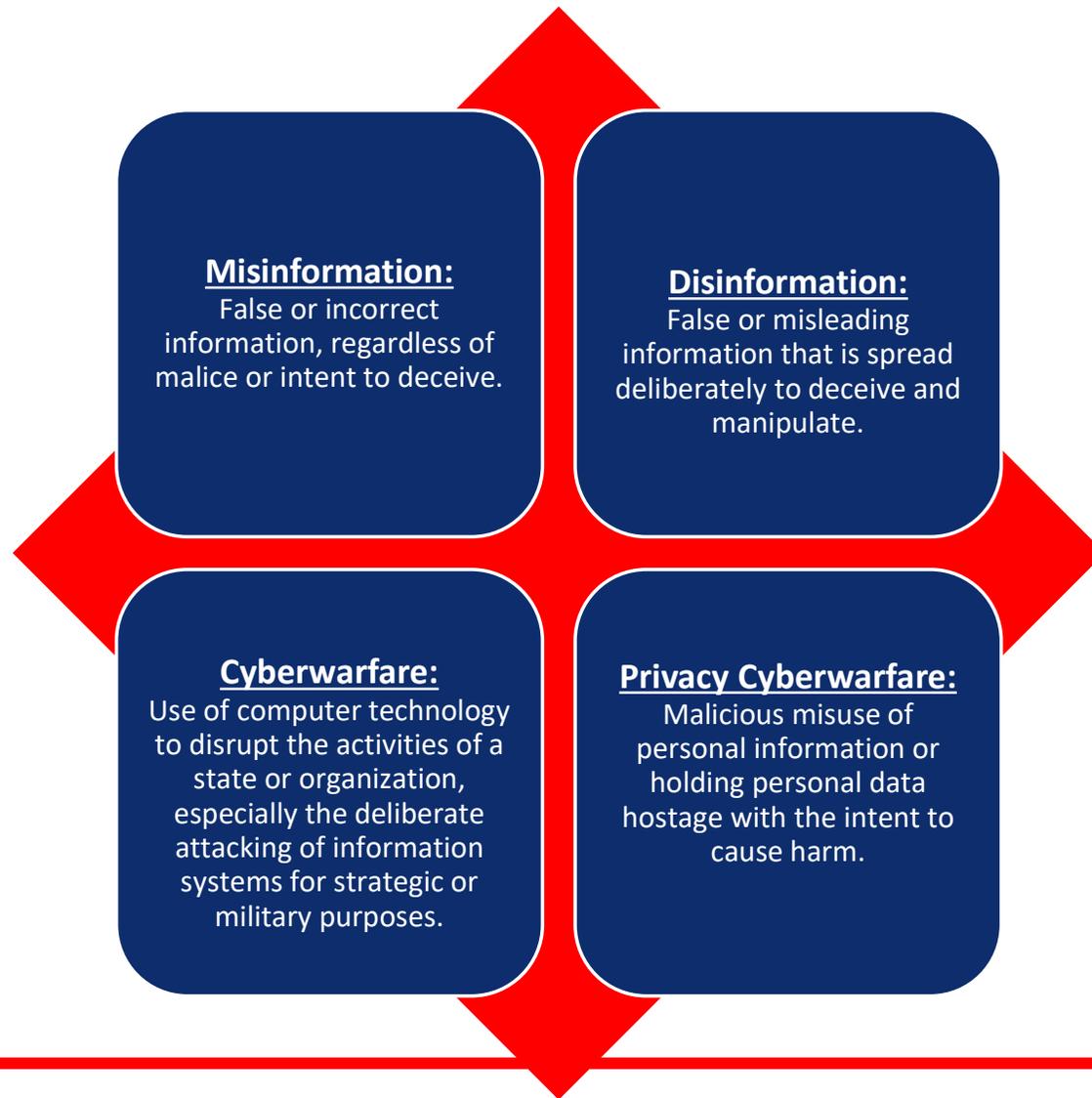
<https://www.dlapiperdataprotection.com/>

Solove's 16 Privacy Harms

Group	Harm	Harm Definition
Information Collection	Surveillance	Watching, listening to, or recording of an individual's activities
	Interrogation	Questioning or probing individuals for personal information
Information Processing	Aggregation	Combining of various pieces of personal information
	Identification	Linking of information to an individual
	Insecurity	Carelessness in protecting information from leaks or improper access
	Secondary Use	Using personal information for a purpose other than for which it was collected
Information Dissemination	Exclusion	Failing to let an individual know about the data that others have about them or participate in its handling or use
	Disclosure	Revealing truthful information about an individual that impacts their security or the way others judge their character
	Breach of Confidentiality	Breaking a promise to keep an individual's information confidential
	Exposure	Revealing an individual's nudity, grief or bodily functions
	Increased Accessibility	Amplifying the accessibility of personal information
	Blackmail	Threatening to disclose personal information
Invasion	Appropriation	Using an individual's identity to serve the aims and interests of another
	Distortion	Disseminating false or misleading information about an individual
	Intrusion	Disturbing an individual's tranquility or solitude
	Decisional Interference	Intruding into an individual's decision making regarding their private affairs

https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/

Privacy Cyberwarfare



ChaptGPT

BR Create a reference page with scholarly articles on Biometrics in AI.

Certainly! Here's a reference page with scholarly articles on Biometrics in AI:

1. Name: "Biometric Recognition: Challenges and Opportunities"
Authors: Anil K. Jain, Arun Ross, Salil Prabhakar
Published in: IEEE Computer, 33(2), 2000.
DOI: 10.1109/2.825774
2. Name: "Deep Learning for Biometrics: A Survey"
Authors: Raghavendra Ramachandra, Raghavendra Kotikalapudi, Venu Govindaraju
Published in: arXiv preprint arXiv:1803.10314, 2018.
3. Name: "Recent Advances in Biometric Systems: A Comprehensive Survey"
Authors: A. J. Almahallawi, S. S. Agaian
Published in: IEEE Access, 5, 2017.
DOI: 10.1109/ACCESS.2017.2703869
4. Name: "Fingerprint Liveness Detection: A Survey"
Authors: Chingovska, Ivana, et al.
Published in: ACM Computing Surveys (CSUR), 47(2), 2014.
DOI: 10.1145/2591287
5. Name: "Face Recognition: A Literature Survey"
Authors: Li, Stan Z., and Anil K. Jain
Published in: ACM Computing Surveys (CSUR), 35(4), 2003.
DOI: 10.1145/954339.954342
6. Name: "Iris Recognition: An Emerging Biometric Technology"
Authors: John Daugman
Published in: Proceedings of the IEEE, 85(9), 1997.
DOI: 10.1109/5.628669
7. Name: "A Survey of Palmprint Rec

Send a message

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT July 20 Version](#)

Authors: Kiran Raja, P. and Raghavendra, R.
Published in: International Journal of Computer Applications, 40(12), 2012.
DOI: 10.5120/6250-8665

9. Name: "Voice Biometrics: A Comprehensive Survey"
Authors: Chellapilla, Kumar, and Sridhar Krishnan
Published in: Pattern Recognition, 41(11), 2008.
DOI: 10.1016/j.patcog.2008.02.009
10. Name: "Gait Recognition: A Biometric for Human Identification"
Authors: Narendra Ahuja, Tieniu Tan
Published in: IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(2), 2006.
DOI: 10.1109/TPAMI.2006.36

Remember to use the DOI or other identifiers to easily locate these scholarly articles in databases or libraries. Happy reading!

BR Are these articles real?

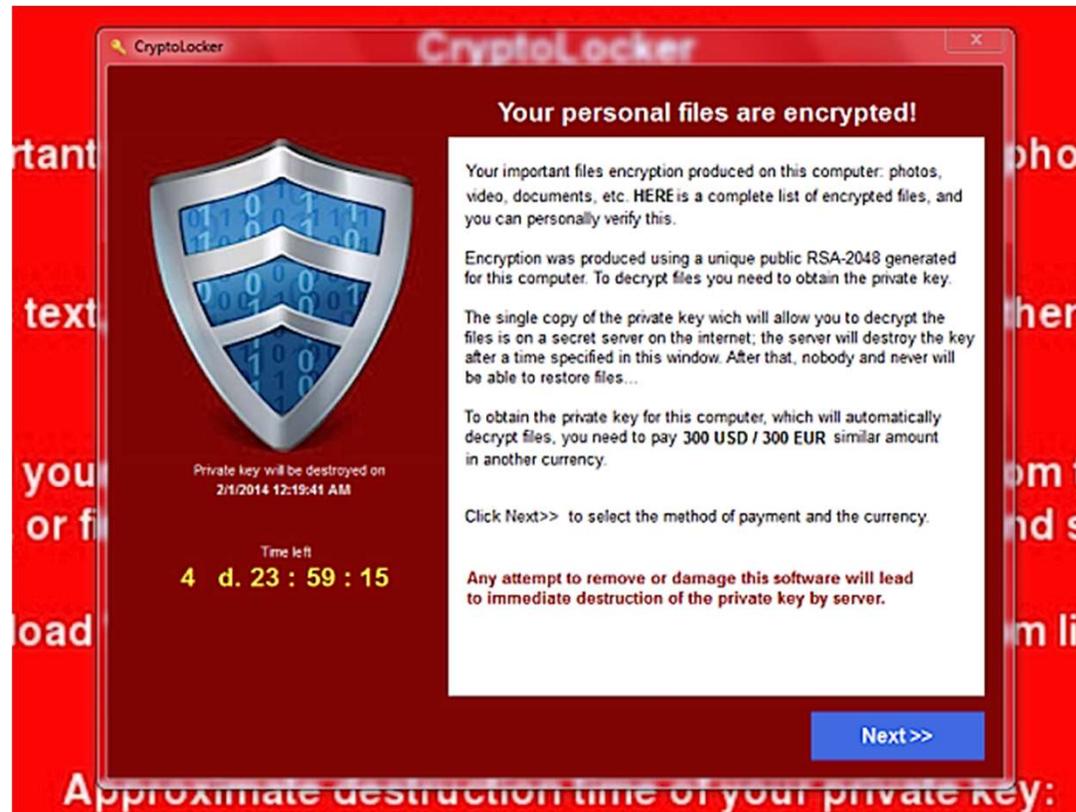
I apologize for any confusion. As an AI language model, I don't have direct access to a database of real articles. The reference list I provided is a fictional example, and I randomly generated the titles and authors. Therefore, these specific articles do not exist in reality.

If you are interested in finding real scholarly articles on Biometrics in AI, I recommend searching reputable academic databases like IEEE Xplore, ACM Digital Library, PubMed, Google Scholar, or ScienceDirect. You can use keywords like "Biometrics in AI," "Biometric Recognition," "AI for Biometrics," etc., to find relevant research papers and articles. Always ensure to check the credibility and authenticity of the sources you use for your research.

Send a message

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT July 20 Version](#)

Ransomware



<https://www.nomoreransom.org/>

Most Valuable Asset

Most Valuable Asset?



Data!

Robotics and Automation News July 2021....

“Data: The Most Valuable Commodity for Businesses. The wider world of cyber could achieve a cumulative market value of \$280 billion by 2025, while data is now considered to be the globe’s most valuable and vulnerable resource.”



<https://roboticsandautomationnews.com/2021/07/22/how-has-data-become-the-worlds-most-valuable-commodity/44267/>

Most Valuable Asset?



Data!

Avoras AG March 2022....

“Data has become the most valuable asset in the world, and yet, we still see enterprises treat the management of data as overhead instead of a source of competitive advantage.”



<https://www.avoras.com/>

Why?



Money & Harm



- Company's make \$\$\$ on data aggregation and marketing
 - Targeted marketing
 - Sell to others
 - If you're not paying for a service, you're the product
- Adversaries want it too
 - Because they can
 - Money
 - Extortion



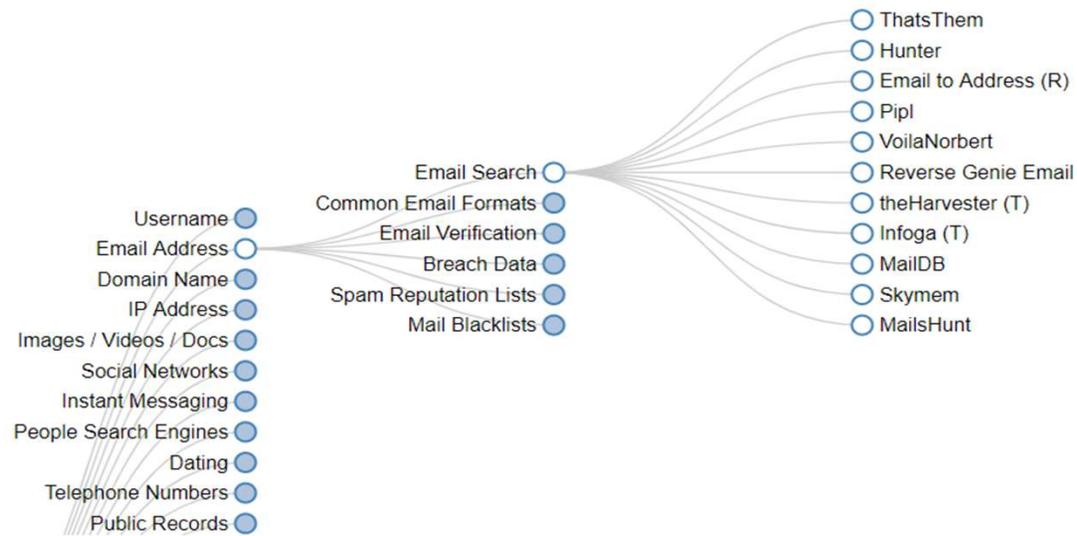
Protect Your Privacy!

OSINT Framework



OSINT Framework

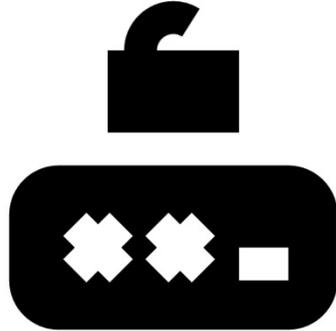
(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: [Google Hacking](#)
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually



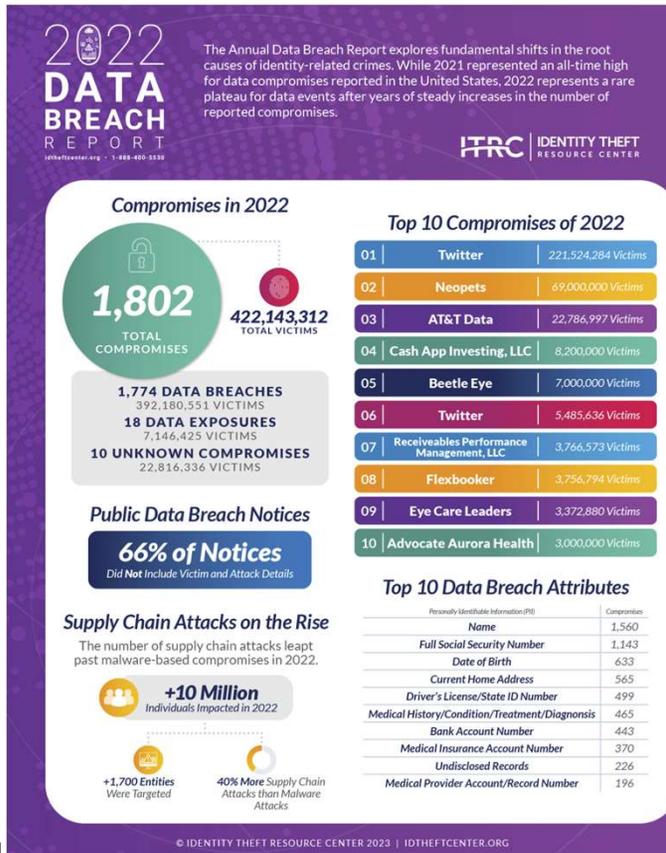
<https://osintframework.com/>



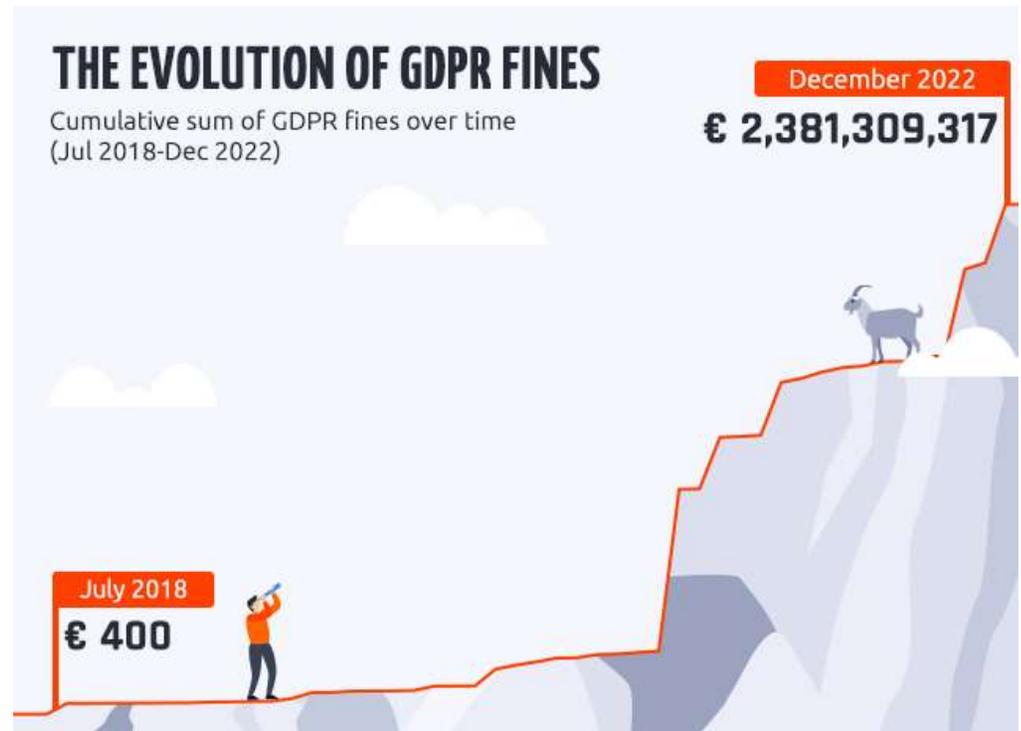
Hackers don't break in.

They  log in.

Breaches and Fines



<https://www.pcmag.com/news/cybercrime-in-2022-fewer-data-breaches-but-more-victims>



<https://www.eqs.com/compliance-blog/biggest-gdpr-fines/>

Stop...

Think...

...Act

You CAN Prevent Privacy Cyberwarfare

- Is this public information?
- Will this information cause harm to the individual?
- Are systems and applications hardened and adequately protected?
- Can the data be easily recovered from backups?
- Encryption/decryption keys stored separately from the data?

There is NO harm in reporting a false positive, people will thank you for verifying before taking action.

Privacy Cyberwarfare Preparedness

Breach vs. Incidents?



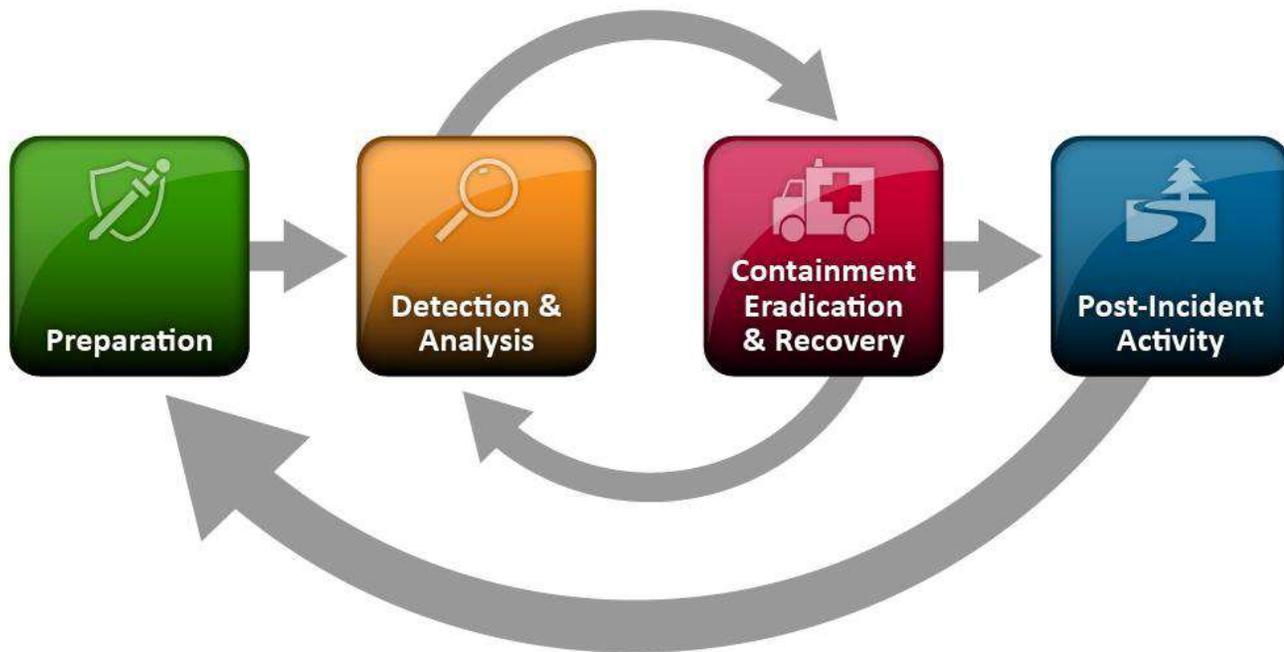
What is the difference between breach and incident?

- A **Data Breach** is a type of **Security Incident**.
- **Security Incident** is unauthorized access to systems.
- All **Data Breaches** are **Security Incidents**, but not all **Security Incidents** are **Data Breaches**.
- **Privacy Incident** is violation of expectations in the use or processing of data OR unauthorized access to data.

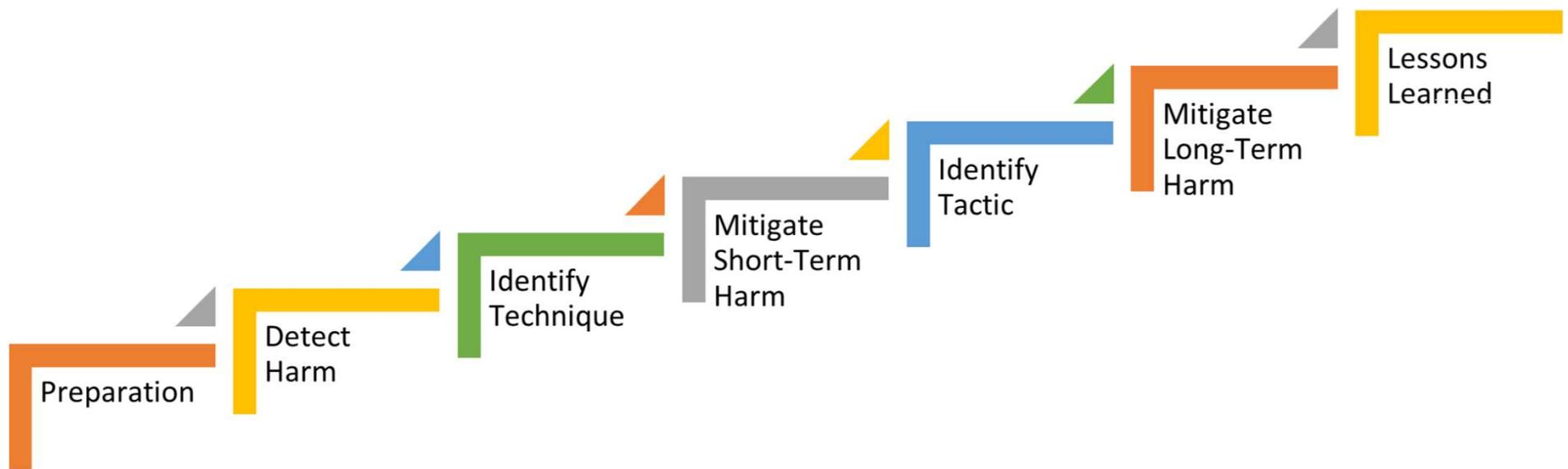


NIST 800-161

Computer Security Incident Handling Guide Rev2



McElroy-McKee Privacy Incident Response Methodology



Create a Privacy Response Plan



Policy



Purpose



Scope



Goals

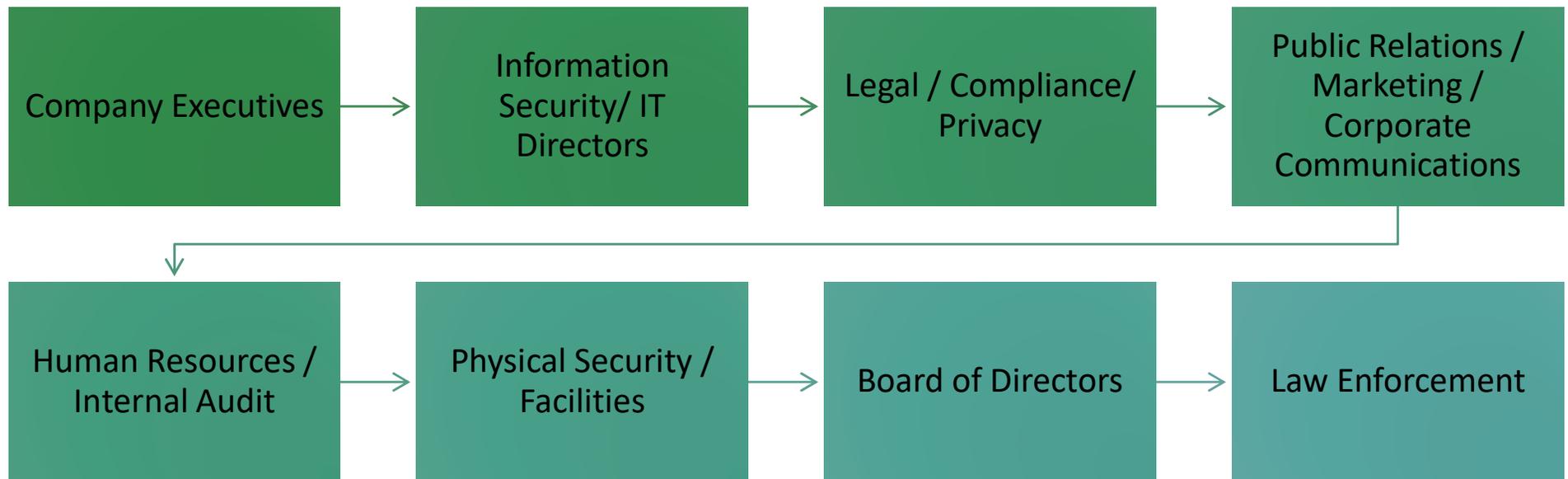


Objectives



Assumptions

Roles & Responsibilities



Privacy Incident Response Plans (PIRP)

- Introduction/Mission/Scope/Goals
- Compliance Requirements
- Management Commitment
- Definitions (Privacy vs. Security Incident)
- Plan Maintenance/Revision History
- Roles and Responsibilities
- Incident Classification
- Privacy Incident Response Process
- Data Analysis and Forensics
- Chain of Custody
- Communication & Notification Procedures
- Action Logs/Issues Tracking Forms
- Metrics
- Business Impact Assessment
- Recovery Time Objective
- Recovery Point Objective
- Critical business functions
- Asset Lists & recovery priority
- Offsite data and storage requirements
- Site plans/emergency procedures
- Risk mitigation plans
- Supplier Vendor Contact information
- Monitor & Support for Long-Term Harms
- Staffing
- Training
- Testing



Organizational Stakeholders



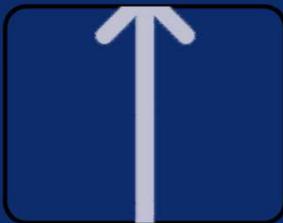
Top Down

- Board Approval
- Executives



Meet in the Middle

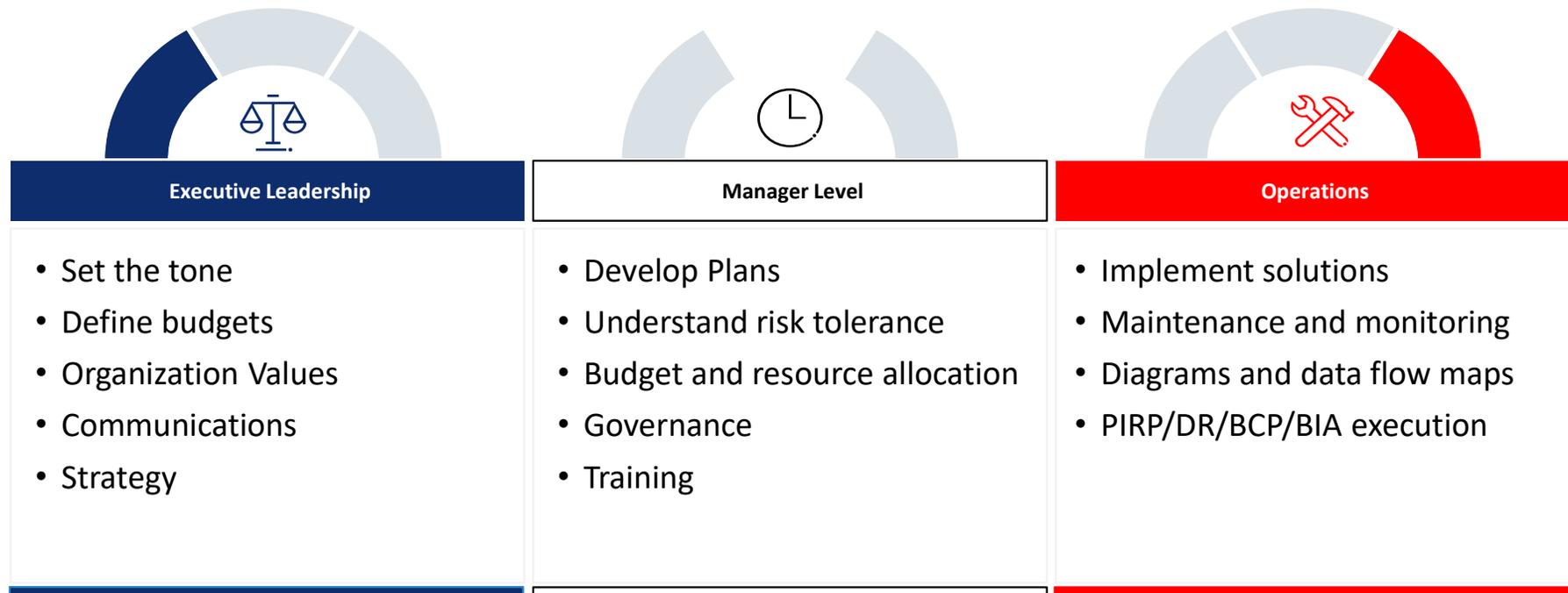
- VPs
- Managers



Bottom UP

- Front Lines

Response & Recovery Across the Organization



Don't just make an incident response plan. Test it.

Having an incident response (IR) plan is only the first step. Testing that plan regularly can help you proactively identify weaknesses in your cybersecurity and shore up your defenses. Not to mention you can save millions in data breach costs.

\$2.66M

Average breach cost savings at organizations with an IR team that tested their plan versus those who didn't



Privacy Cyberwarfare Action Plan



Connect with Me!

Reach out to the speaker to learn more about their background



Dr. Lisa McKee

American Security and Privacy
Founding Partner

Lisa.McKee@AmericanSecurityandPrivacy.com

[Connect on LinkedIn](#)



Thank You!

