

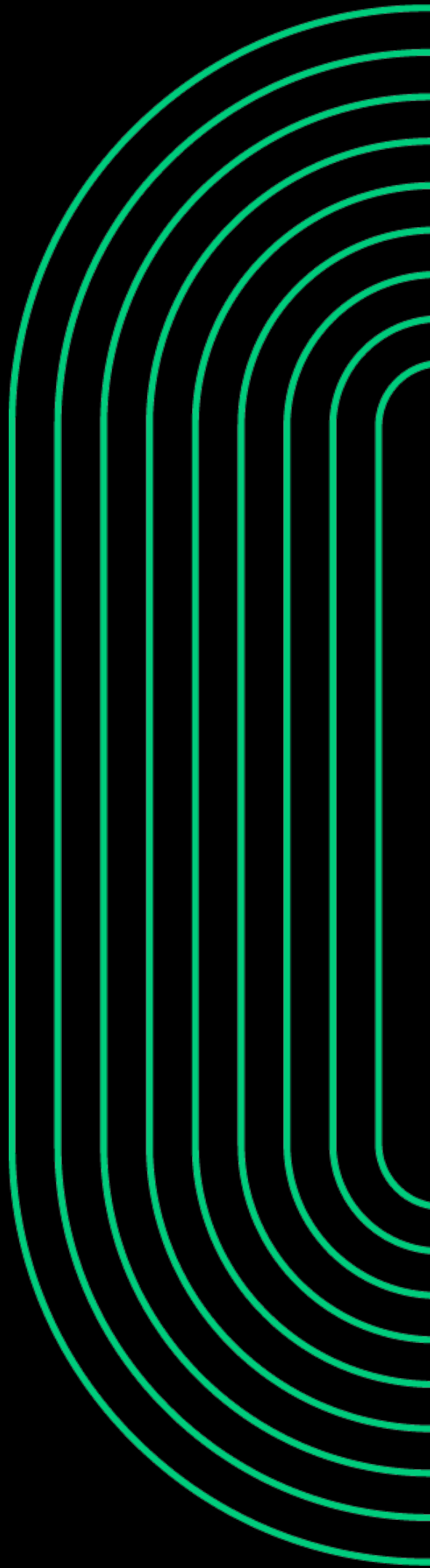


Don't Say the "B" Word: Data Events, Incidents and Breaches

Presenter:

Ilya Smith
Senior Attorney
Clark Hill
+1 313.309.9466 (office) | + 312.517.7572 (fax)
ismith@clarkhill.com | www.clarkhill.com

April 2024



AGENDA

1

- Cybersecurity and Privacy Trends for K-12

2

- Statutory Breach Notification Framework

3

- Incident Response Do's and Don'ts

4

- Risk factors for targeting

5

- Questions



Why is This Important?

As an education administrator you may rank (1) avoiding disruption to operations, (2) loss of trust, (3) financial cost among the top of your list

◆ WSJ NEWS EXCLUSIVE | NATIONAL SECURITY

SolarWinds Hack Victims: From Tech Companies to a Hospital and University

A Wall Street Journal analysis identified at least 24 organizations that installed software laced with malicious code by Russian hackers

The New York Times

Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.

The New York Times

Google Is Fined \$57 Million Under Europe's Data Privacy Law



TECHNOLOGY

After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users



General Data Security & Privacy Trends



Department of
Education and
State Regulator
Incident
Notification




Data Subject
Rights &
Access
Requests



Employee and
Third Party
Data Collection



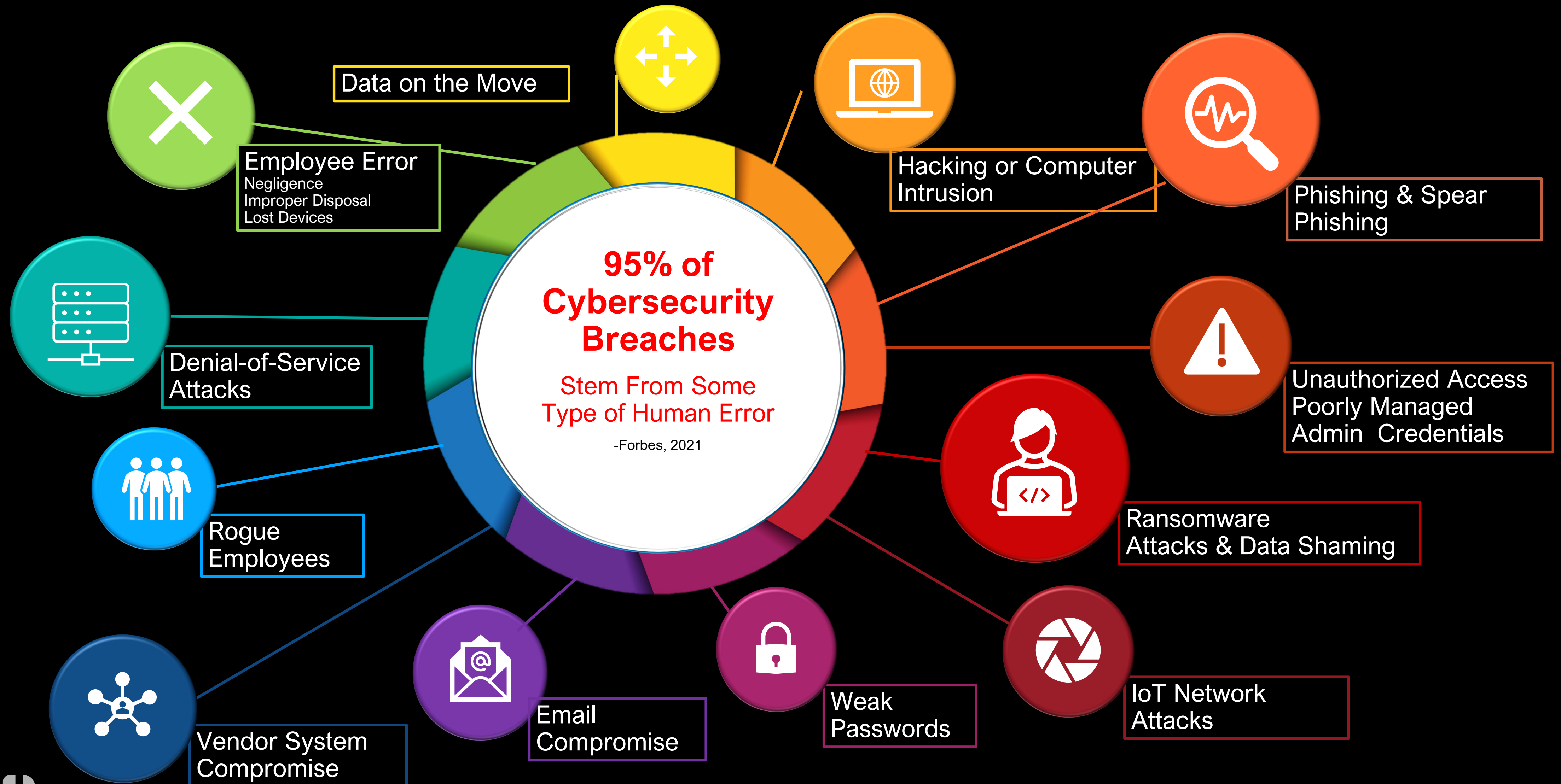
Cyber Warfare



Artificial
Intelligence &
Machine
Learning



Cybersecurity Threat Landscape



The State of K-12 Cybersecurity Year in Review Report (2022)

Levin, Douglas A. (2022). "The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report." K12 Security Information Exchange (K12 SIX). Available online at: <https://www.k12six.org/the-report>

Since 2016, K12 SIX has cataloged a **total of 1,331 publicly disclosed school cyber incidents (1 incident per school day)** affecting U.S. school districts (and other public educational organizations) including the following incident types:

- Student data breaches
- Ransomware attacks
- Denial of service (DoS) attacks
- Online class and school meeting invasions
- Data breaches involving insiders
- Business email compromise (BEC) scams
- Website and social media defacement

Of the total reported breaches, 55% are attributable to vendors, nonprofit and government partners; and 14% are due to staff errors.



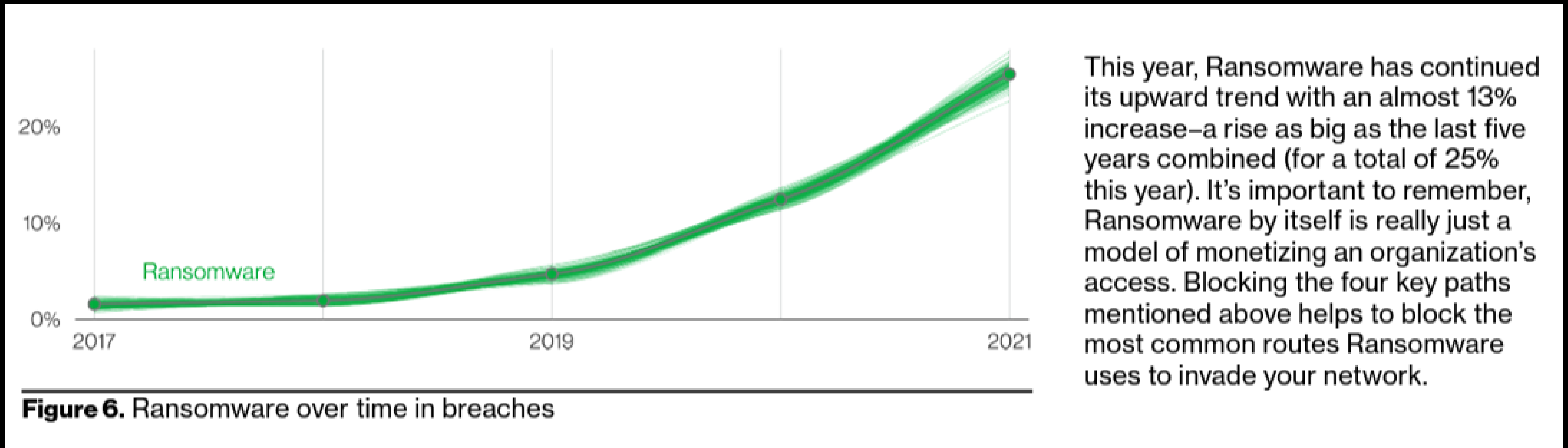
The State of K-12 Cybersecurity Year in Review Report (2022)

Levin, Douglas A. (2022). "The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report." K12 Security Information Exchange (K12 SIX). Available online at: <https://www.k12six.org/the-report>

Since 2016, K12 SIX has cataloged a **total of 1,331 publicly disclosed school cyber incidents (1 incident per school day)** affecting U.S. school districts (and other public educational organizations) including the following incident types:

- Student data breaches
- Ransomware attacks
- Denial of service (DoS) attacks
- Data breaches involving insiders
- Business email compromise (BEC) scams
- Website and social media defacement

Is Ransomware Still an Issue?



How Much is Personal Information Worth on the Dark Web?



Stolen PayPal account details,
minimum \$100 balance
\$10



Hacked Gmail account **\$65**



Hacked Facebook account
\$45



Netflix account,
1-year subscription
\$25



New York driver's license
\$70

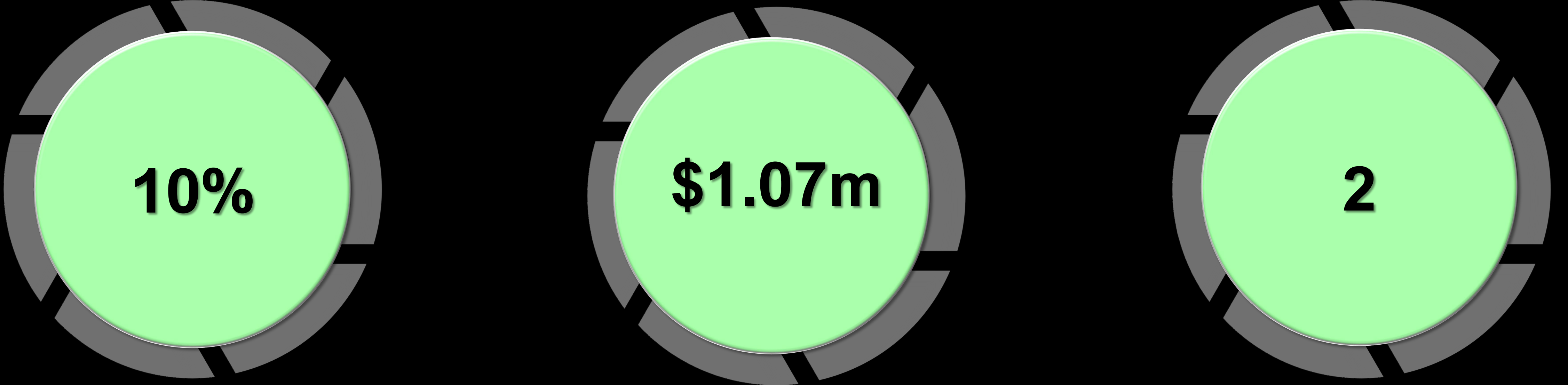


Credit Card Data, with account
balance up to 5,000
\$120



Various European Union
passports
\$3,800

What is the cost of ransomware and other breaches



10%

Increase in average total cost of a breach, 2020-2021

\$1.07m

Cost difference where remote work was a factor in causing the breach

2

Consecutive years US education sector had the highest occurrence rate of ransomware attacks



“For the second calendar year running, at least 75 percent of all data breach incidents affecting U.S. public K-12 school districts were the result of security incidents involving school district vendors and other partners... the most significant vector of data breaches impacting education settings – in terms of numbers of individuals affected – are education tech vendors and other trusted non-profit and government partners.”

”

[The State of K-12 Cybersecurity: Year in Review - 2022 Annual Report](#)



2

Privacy and Security Legal Framework

Michigan Data Breach Notification Statute and FERPA

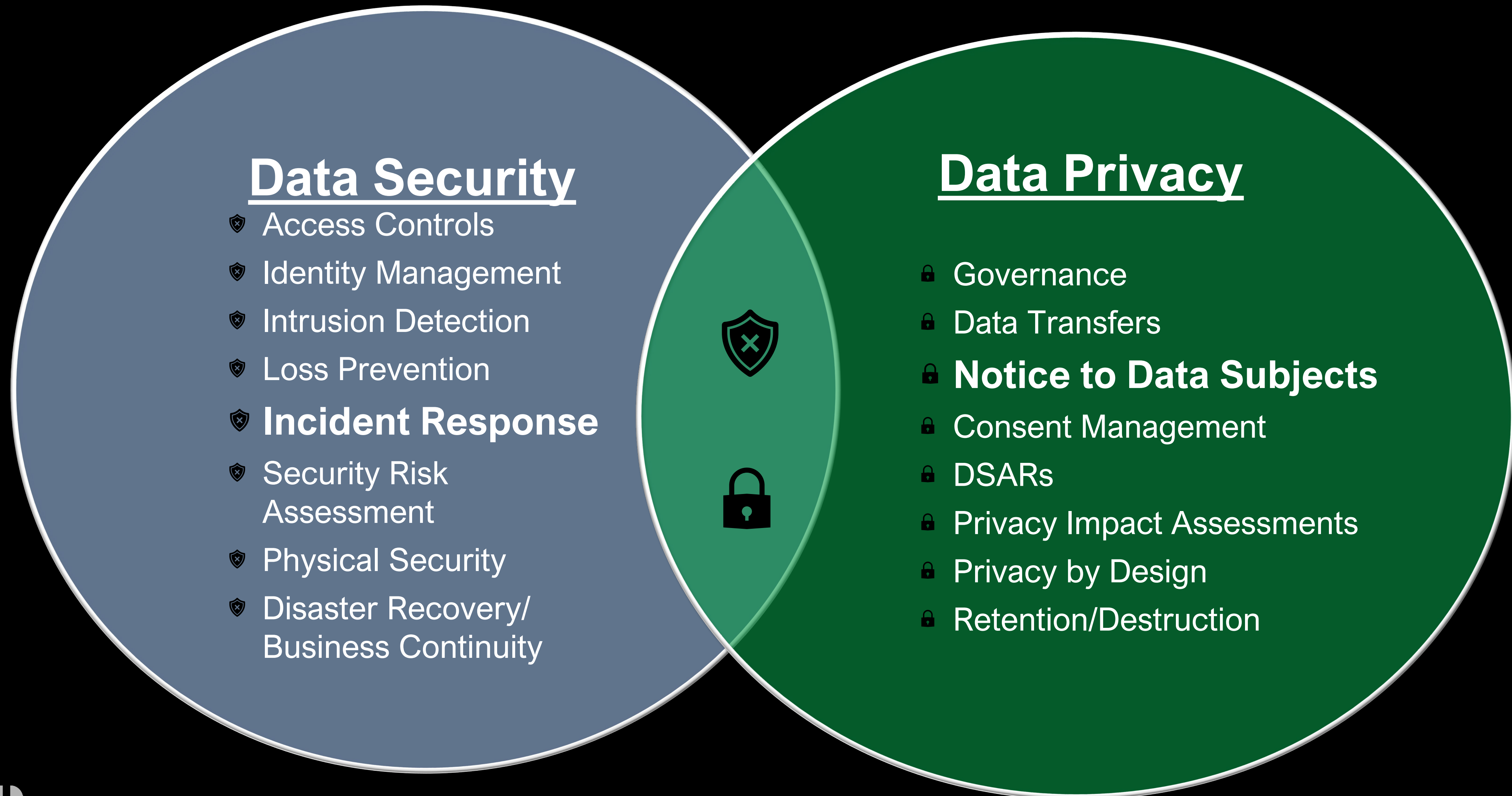
Obligations following an unauthorized disclosure of PII/Education Records, Mich. Comp. Laws §§ 445.61, 445.63, 444.64, 445.72 and 34 CFR Part 99

- **Words matter: Notification to impacted individuals per state law is triggered upon a determination of a BREACH (see Legal Framework Handout).**
- **Breach:** A legal term of art, requires legal analysis taking into account—nature of data, security measures in place, impacted individuals, reason for collection, authorized parties, FERPA disclosure exceptions, contractual obligations, access and acquisition, risk of harm and more
- **Security Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies **Source:** [NIST SP 800-82r3](#) under Incident from [FIPS 200](#)
- US DOE does not have the authority under FERPA to require that agencies or institutions issue a direct notice to a parent or student upon an unauthorized disclosure of education records. FERPA only requires that the agency or institution record the disclosure so that a parent or student will become aware of the disclosure during an inspection of the student's education record.



Data Security vs. Data Privacy?

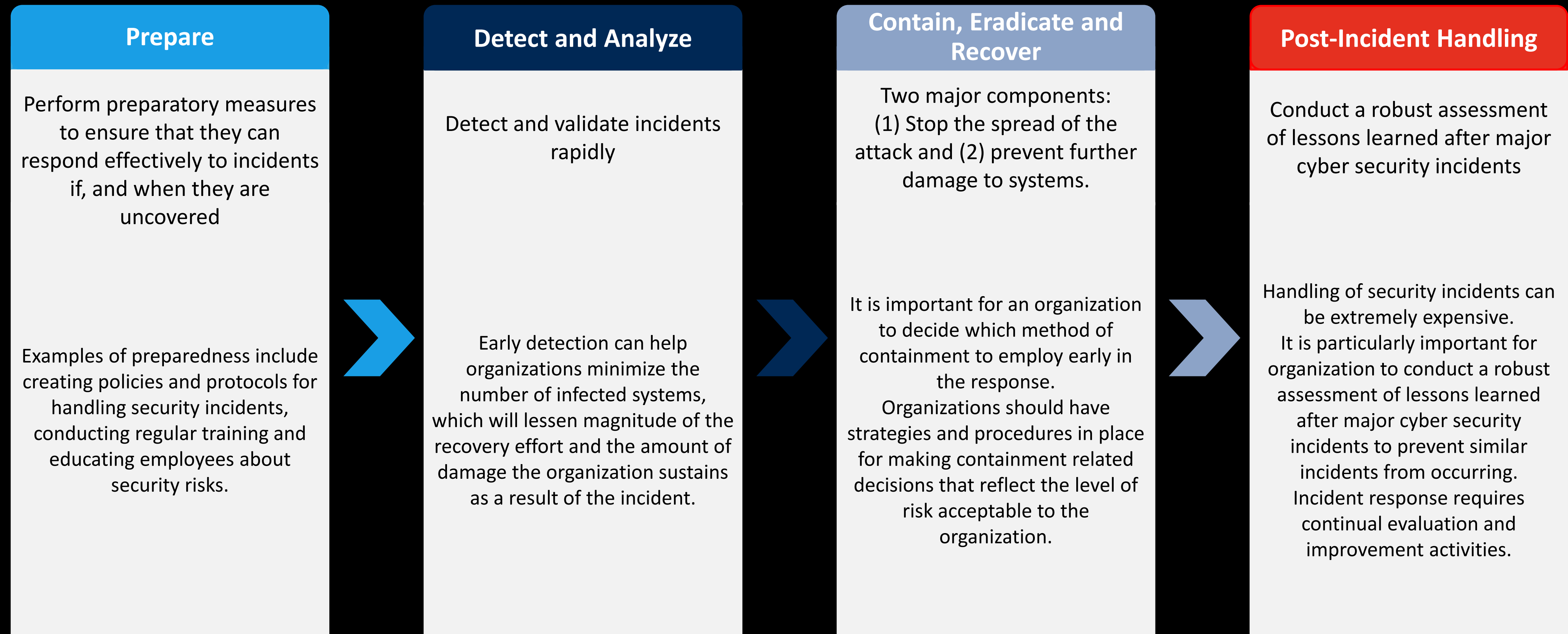
Similarities & Differences



3

Incident Response

Incident Response Framework (NIST)



Incident Response Do's and Don't's—Prepare

Policy, IRP, and Procedures.

DO make security the responsibility of every staff person.

DO require the immediate reporting of suspicious activities or potential incidents : Do your employees know what to look for and who to report it to?

DO NOT expect your IRT to be ready without testing and scenario-based playbooks.

DO develop Muscle Memory and conduct post mortems to draw from past incident response and tabletop lessons learned.

Communications.

DO make pre-vetted communications templates available and **DO** expect that each of your constituencies may be impacted and need updates; **DO NOT** make premature notifications or communications. **DO** plan for out of band communications in an incident response.



Incident Response Do's and Don't's (Prepare con't)

Business Continuity Planning.

DO validate backups for integrity, availability and accessibility;

DO know gain a clear understanding of business-critical facilities, systems, communication channels, processes, and data.

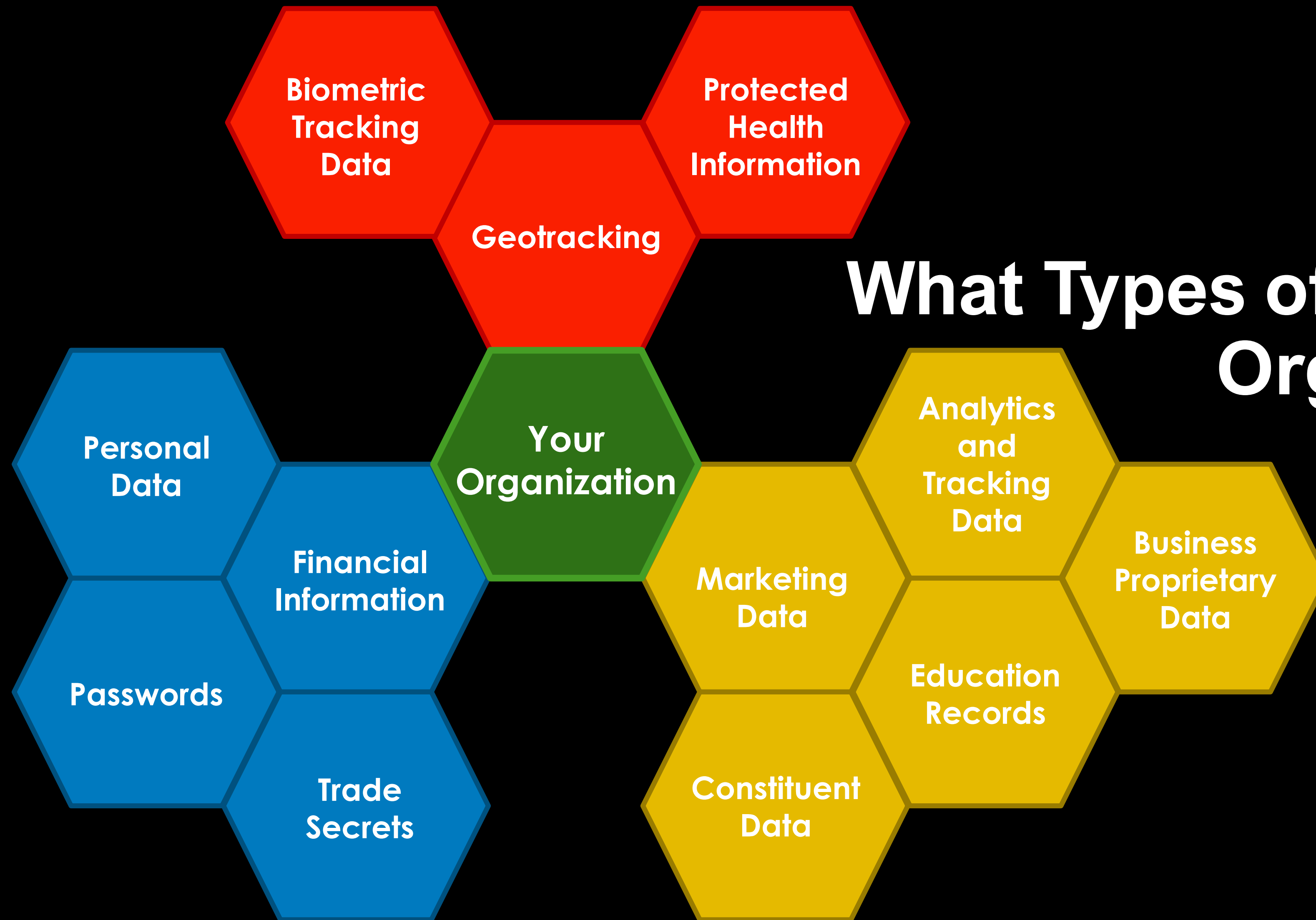
Data Mapping and Hygiene.

DO understand what type of data you (and others on your behalf) collect and process and where it resides. **DO NOT** over retain data with PII; encrypt at rest and in transit.

Resources.

DO make sure trusted partners and breach coach are available and contracts are in place. If you have cyber insurance, **DO** understand who is insurance “approved” to provide services. **DO NOT** assume that your existing vendors are the right teams to conduct investigation or forensics.





What Types of Data Does Your Organization Hold?

What do you do with that data?



Incident Response Do's and Don'ts—Detect & Analyze

Role of IRT and Incident Commander. **DO** make duties and roles for IRT clear; they may look and feel different than normal duties. IRT Authority and Charge should be established or asserted.

Scope of Response. **DO** understand that there will be several parallel workflows and that different SMEs will need to own and/or participate in various parts of a response.

Escalation/Severity. **DO** apply IRP protocols and incident classification.

Documentation. **DO** plan and enforce who and how performs documentation of investigation (facts only) and legal analysis (and preserve attorney-client privilege), **DO NOT** allow for organic notetaking and **DO NOT** circulate or make available confidential or privileged communications.

Evidence Gathering. **DO** ensure secure and chain of custody process to evidence collection (i.e. access logs etc.) for forensics review.

Resources. **DO** determine within first 24 hours, how and when to leverage insurance carrier, breach coach, outside counsel, forensics vendors, communications/PR assistance, and/or coordination with the various law enforcement agencies.



Incident Response Do's and Don'ts—Contain, Eradicate and Recover

Containment/Eradiation.

DO assess if a containment plan or eradication (e.g. password change; endpoint monitoring; disconnect and isolate machines) is necessary. **DO stop the bleed.**

Recovery.

DO NOT recover from contaminated backups. While backups may address restoration, DO understand double extortion possibilities: encryption key AND non-disclosure of PII already exfiltrated.

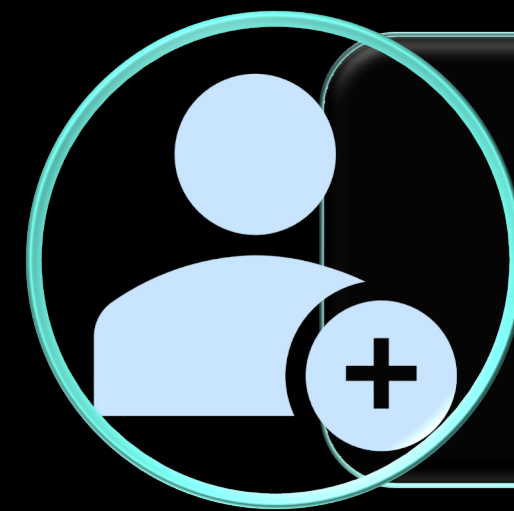
Notifications and Disclosures.

DO understand that investigations and breach determinations (including impacted individuals and data) take time. MI State Breach Notification Laws take that into account and the timing and adequacy of notice is dependent on an investigation's completeness.

DO understand that just because you don't have to, sometimes its still the right thing to do.

Lessons Learned. **DO NOT** repeat the same mistakes. If vulnerabilities or gaps in process or policy are discovered; **DO address gaps in security controls.**





Risk Factors and Key Takeaways

Risk Profile and Management

According to K12 SIX, data from reported incidents in 2016-2021 suggests that some of you are more likely to be a target of cyberattacks: Larger student enrollment districts and Districts serving wealthier populations attract sophisticated Threat Actors

Researchers caution though, that all districts are at risk and to focus attention to reducing the threat profile and implementing third party vendor/partner data sharing controls:

1. Do you conduct privacy and security **Due Diligence** on potential vendors and partners
2. What is your approach to **Risk Tolerance and Management** (risk avoidant, risk sharing, risk transferring, risk mitigation)
3. Is **Insurance** in place to finance risk?
4. Contractual Obligations and **DPAs (i.e. non disclosure and use limitation, breach costs and notice, security safeguards, insurance, retention and destruction, “other school official” designation)**
5. Have you agreed to adequate **data minimization and security controls?**



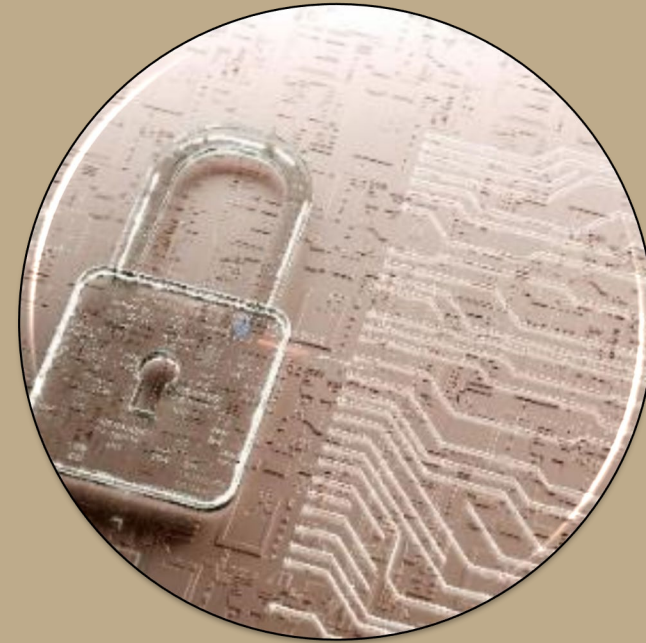


Key Takeaways

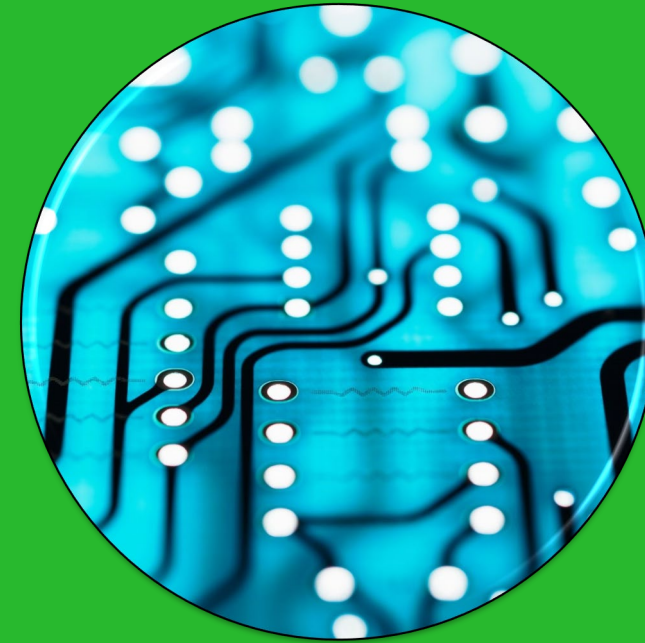
Information Security - Best Practice Considerations



Incident
Response Plan
Development
and Training with
Key Leaders



Assess Your
Administrative,
Technical and
Physical Controls
(ATP's)



Evaluate Third-
Party
Infrastructure



Regular Auditing
and Testing



Review your
Incident
Response Plan



Best Practice Considerations for Shrinking your Privacy Threat Surface



Know Your Data



Understand
Your Data Flow



Ed Tech and
Vendor Risk
Management



Incident
Response Plan
& Prep



Privacy by
Design





Questions?



Thank You

Legal Disclaimer

This document is not intended to give legal advice. It is comprised of general information. Employers facing specific issues should seek the assistance of an attorney.