

# WV BOARD OF RISK AND INSURANCE MANAGEMENT



## Board of Education Cyber Liability and Awareness

July 16, 2020

WVDE Office of School Finance Conference

# Agenda

- Overview of BRIM
- Understanding the Threat
- Cyber Liability Policy
- Privacy and Security Incident Reporting
- Resources
- Q & A

# OVERVIEW OF BRIM



# Overview of BRIM

- **ENABLING STATUTE:** *WV Code §29-12-1 et seq.*
- Created by WV Legislature in 1957 as the agency to secure reasonably broad protection against liability arising from state activities and responsibilities, and loss or damage to state property, through insurance coverage, claims management, and promotion of principles of loss control and risk management.
  - Pursuant to §29-12-5, BRIM determines the kinds of coverage and limits needed, as well as the conditions, limitations, exclusions, deductibles and endorsements for state insurance.

# BRIM procures coverage for the following:

- General liability
- Automobile
- Wrongful acts liability
- Professional liability
- Personal injury liability
- Stop gap liability
- Property
- Cyber liability
- Aviation
- Boiler/HVAC, and
- Statutory bond, in addition to excess liability coverage for County Boards of Education as required by statute

# BRIM's loss control activities include:

- Annual insurance loss prevention inspections on selected state structures of significant insurable risks to determine exposures present that may result in a claim;
- Recommendations to eliminate/reduce opportunities for claims;
- Establishing loss prevention standards;
- Providing opportunities for credits against premiums by minimizing losses; and
- Providing loss control education through public information presentations.

# BRIM and the State Privacy Office

- Through the State Privacy Office, BRIM supports and guides state agencies' efforts to mitigate loss by:
  - Identifying data privacy risks;
  - Proactively protecting sensitive information; and
  - Safeguarding the privacy of personal information, including protected health information, that is collected, used, disclosed and maintained by the State.

# Overview of BRIM

BRIM has 26 full-time employees:

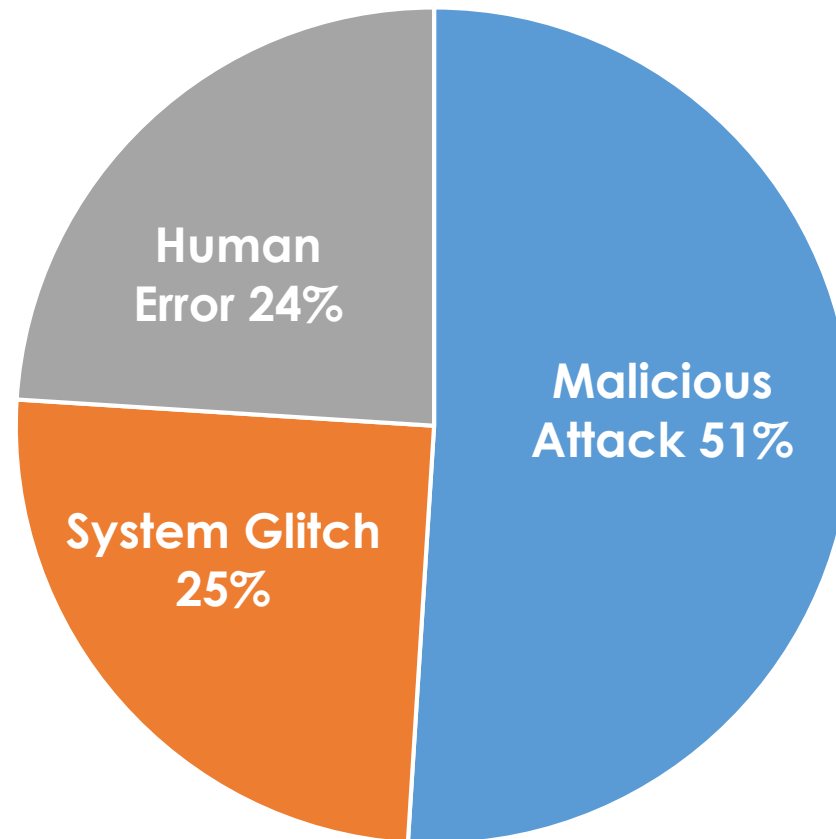
- 4 Underwriting
- 8 Claims
- 5 Loss Control
- 4 Finance
- 2 Administration, and
- 3 Privacy Office



# UNDERSTANDING THE THREAT




# Root Causes of a Data Breach: United States Distribution of Benchmark Sample



<sup>10</sup>Source: Ponemon Institute, 2019  
Cost of Data Breach Study, United  
States

# Malicious or criminal attack

- Ransomware
  - Phishing Attack
  - Social Engineering
  - Spoofing
  - Malware
    - Adware – continual ads and pop-up windows
    - Password Stealers
    - Virus – replicates itself and negatively impacts system functionality
  - Backdoor – exploits security vulnerabilities
  - Distributed Denial of Service (DDoS)
- 

Source: <https://leapfrogservices.com/worm-virus-malware-phishing-spoofing-hacking-phreaking-spyware-whats-what-cybercrime-lingo-deciphered/>

# HUMAN ERROR

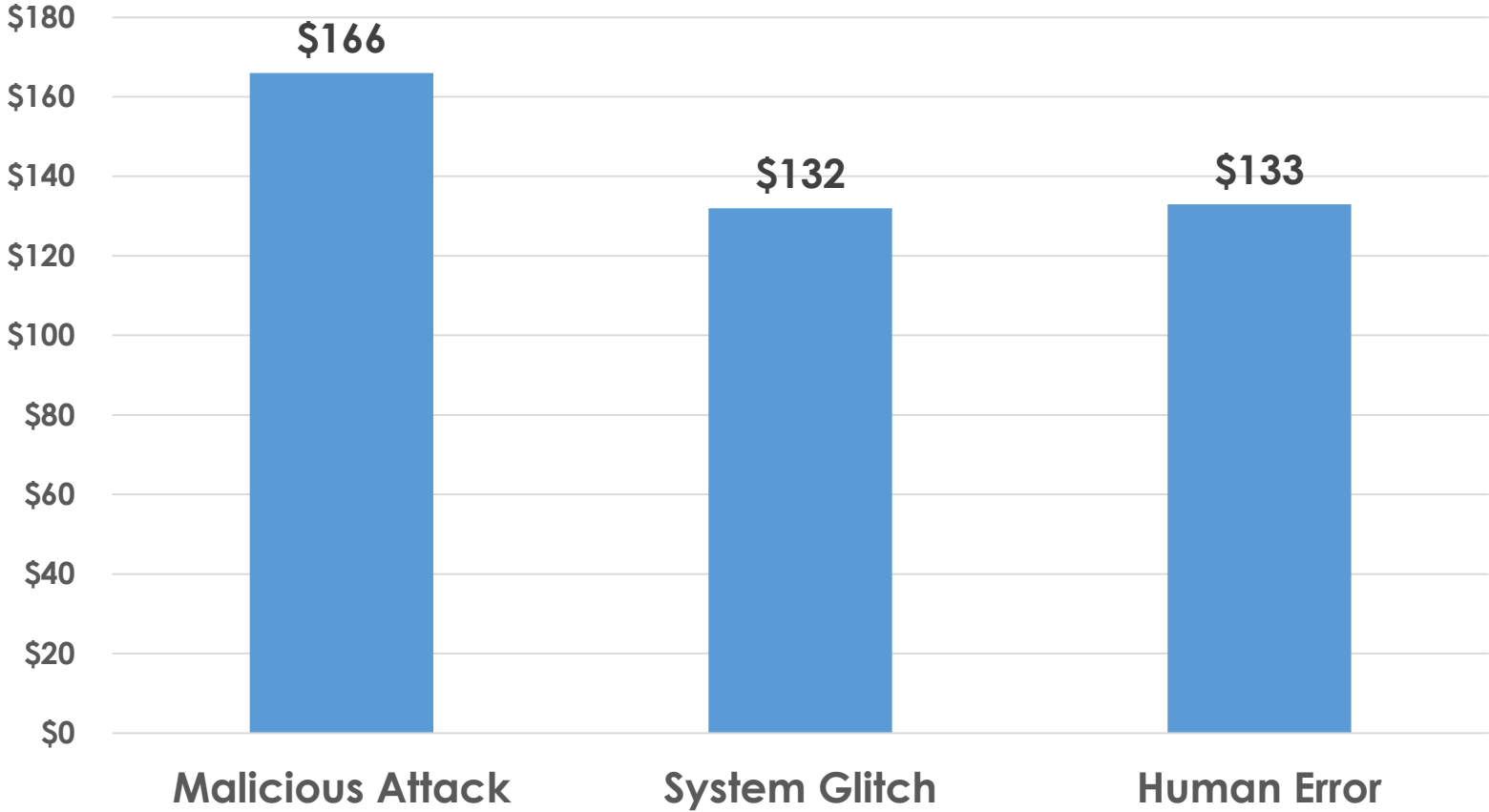
- Sending mail to the wrong address
- Sending email to the wrong person
- Loss of paperwork or unsecured devices
- Improper storage or disposal of records
- Careless verbal discussions
- Not following policies and procedures
- Failure to redact protected information

# System Glitches

- Application errors
- Inadvertent data dumps
- Logic errors in data transfer
- Identity or authentication failures (wrongful access)
- Data recovery failures

Source: <https://www.infosecurity-magazine.com/news/human-error-and-system-glitches-drive-nearly-two/>

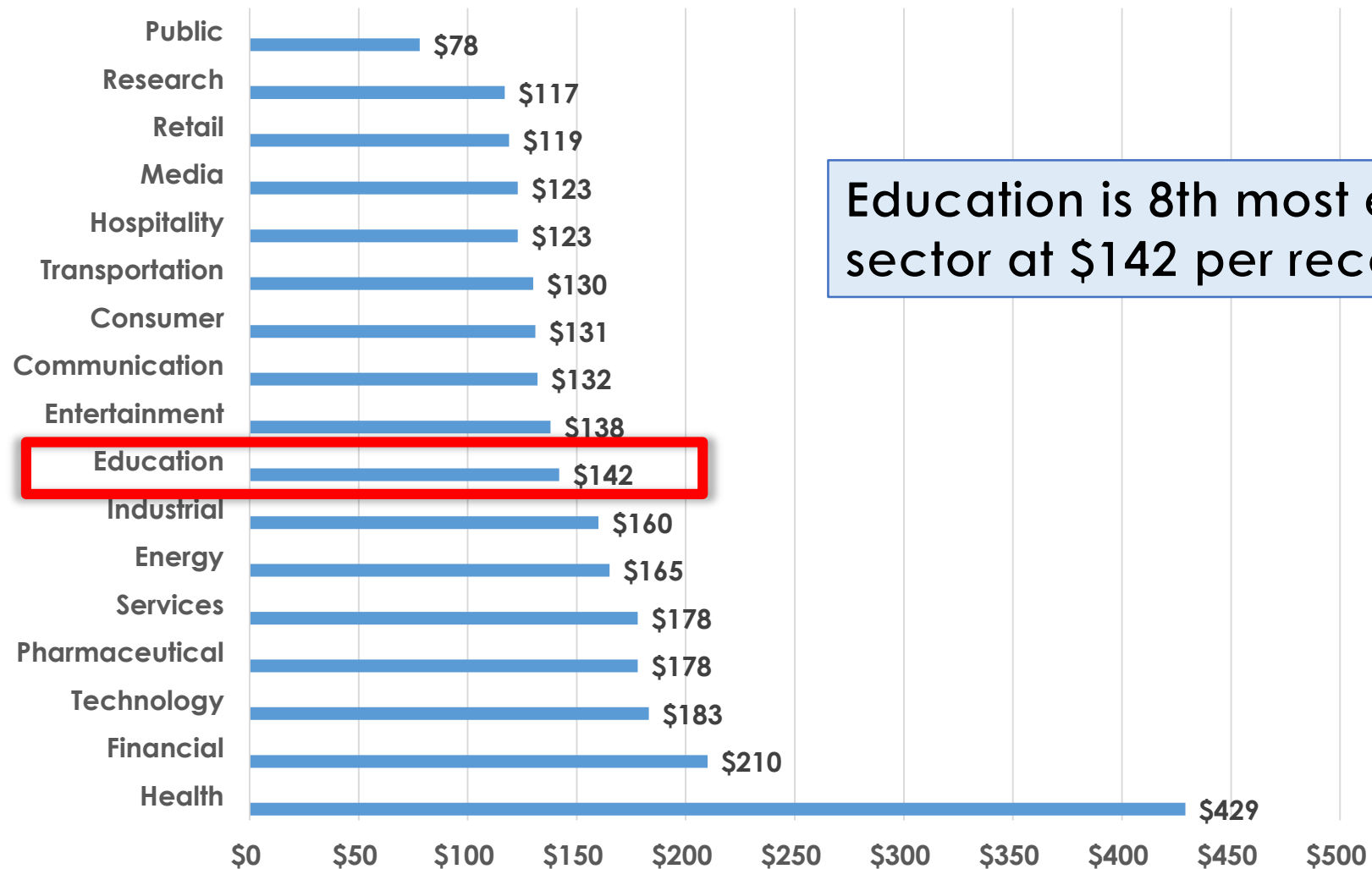
# Per Capita (Record) Breach Cost by Root Cause: United States



<sup>10</sup>Source: Ponemon Institute, 2019 Cost of Data Breach Study, United States

# Per capita Cost by Industry Sector

Source: Ponemon 2019 Cost of a Data Breach Report



Education is 8th most expensive sector at \$142 per record.

# Education Tech- Focus on K-12

by Micah Castelo, June 17, 2020

- Cyber incidents reported by U.S schools and districts in in 2019: **348**
- Nearly **a threefold increase** above the number of incidents in 2018.
- Education is seen as easy targets by cyber attackers.
- Lack of resources and security funding.
- Vast majority of attacks occur through social engineering- phishing emails.

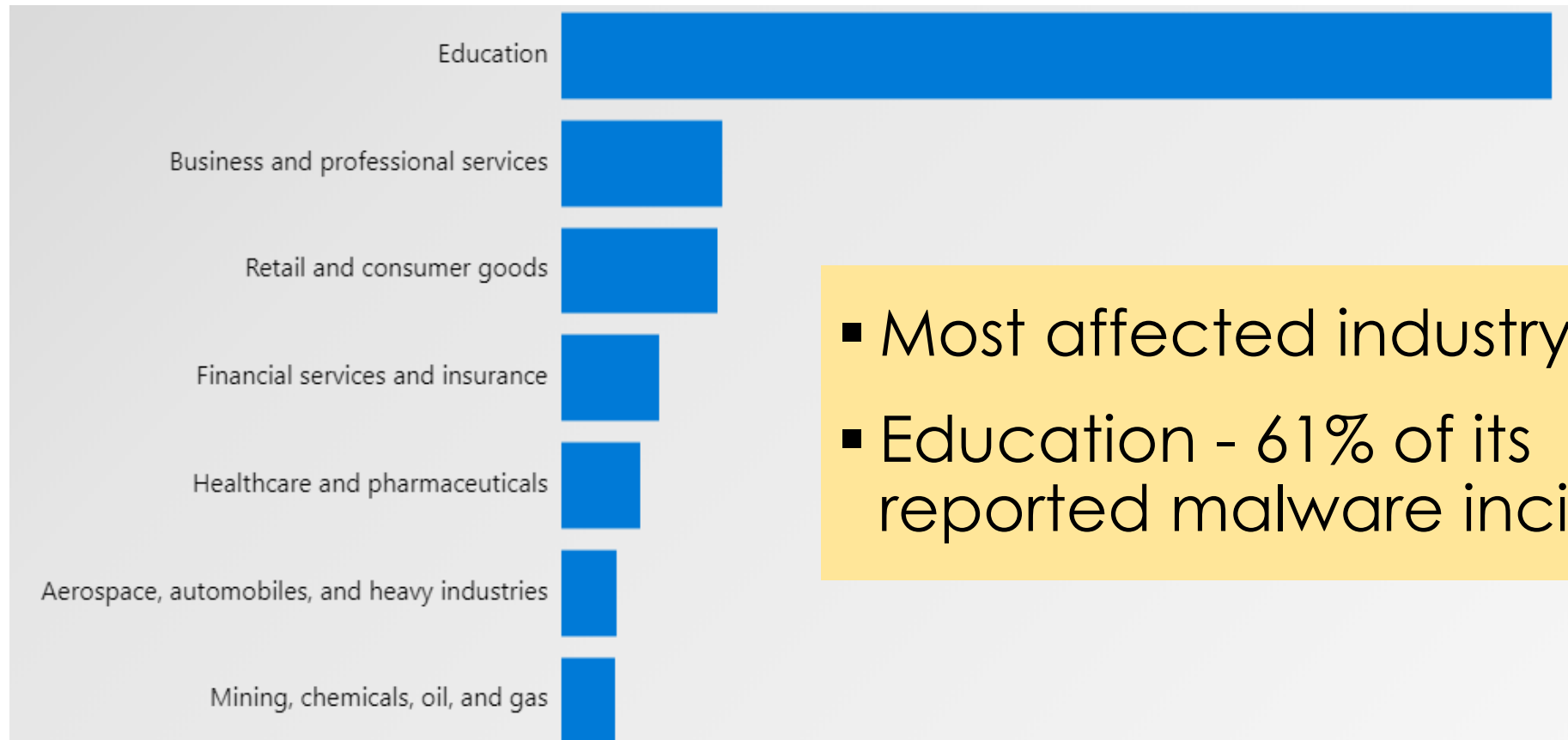
<https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon>



# Education Tech- Focus on K-12

by Micah Castelo, June 17, 2020

Microsoft Security, Global enterprise malware encounters: **last 30 days, June 2020**



- Most affected industry.
- Education - 61% of its reported malware incidents.

Home » Cybersecurity » SBN News » Child Identity Thief Receives 259 Months in Federal Prison after Running a \$3.3 Million Scheme

## Child Identity Thief Receives 259 Months in Federal Prison after Running a \$3.3 Million Scheme

 by Alina Bizga on July 3, 2020

<https://securityboulevard.com/2020/07/child-identity-thief-receives-259-months-in-federal-prison-after-running-a-3-3-million-scheme/>

## 121 children's identities stolen in massive nationwide fraud, auto theft ring; 20 arrested by LSP



Updated: 5:17 PM CDT Jul 1, 2020

147  
Shares



WDSU Digital Team

<https://www.wdsu.com/article/121-childrens-identities-stolen-in-massive-nationwide-fraud-auto-theft-ring-20-arrested-by-lsp/33025146>

# Identity Theft Resource Center: Facts about Child Identity Theft

- Children often do not become aware that identity is stolen until after age 18 and establishing credit.
- Quotes the Javelin Strategy & Research 2018 Child Identity Fraud Study:
  - > 1 million child identity thefts in 2017
  - 60% of child identity thefts occurred by someone known to the child

# Cyber Liability Policy



Insurer: AIG Specialty Insurance Company

# Limit of Liability/Coverages

- \$25 Million Aggregate with \$6 million per county Board of Education limit
- \$50,000 Deductible (BRIM) - \$2,500 per occurrence deductible for each Board of Education

# Coverages

- Media Content Coverage

Resulting from wrongful act claims - Act, error, omission, negligent supervision, misstatement made by insured.

- Plagiarism
- Invasion of rights of privacy or publicity
- Defamation, libel, slander, product disparagement
- Wrongful entry or eviction, trespass, eavesdropping of other invasion of right to private occupancy, false arrest, malicious prosecution
- Negligent or intentional infliction of emotional distress

# Coverages

- Security and Privacy Coverage

**Security Failure** – failure or violation of the security of a computer system

**Privacy Event** – failure to protect confidential information (whether by phishing or other social engineering technique)

- Network Interruption Coverage - 12 Hour waiting period

Material Interruption – actual and measurable interruption or suspension of business caused by Security Failure

# Coverages

- Event Management Coverage

Coverage applies solely with respect to Security Failure or Privacy Event.

- Forensic Investigation
- Public Relations
- Crisis Management
- Notification services
- Identity theft services
- Restoration, recreation or recollection of electronic data



# Coverages

- Cyber Extortion Coverage

Coverage applies solely with respect to Security Threat or Privacy Event.

**Security Threat** – any threat or connected series of threats to commit an intentional attack against a computer system for the purpose of demanding money, securities or other tangible or intangible property of value from the insured.

**Privacy Threat** – any threat or connected series of threats to unlawfully use or publicly disclose “Confidential Information” misappropriated from the insured for the purpose of demanding money, securities or other tangible or intangible property of value from the insured.

# Coverages

- Reputation Guard Coverage – Limit \$50,000

Coverage applies solely with respect to Reputation Threat or Reputation Attack and Insurer will pay Proactive Costs.

**Reputation Threat** – any act or event by a third party that the insured believes would, if disclosed, be seen as a material breach of trust to customers, employees and have an adverse impact on public perception of the insured.

**Reputation Attack** – any publication by a third party that the insured believes will be seen by insured's stakeholders as a material breach of trust and have an adverse impact on the insured.

**Proactive Costs** – consultation costs incurred in connection with a Reputation Threat prior to the earlier of:

1. a Reputation Attack arising out of the subject Reputation Threat, or
2. the 90<sup>th</sup> day after a PR firm is hired in response to the Reputation Threat.

# Privacy and Security Incident Reporting



# Recognizing a Data Privacy Incident

- **FERPA (34 CFR § 99.3):**

The *unauthorized* disclosure or access of the Personally Identifiable Information (PII) of **students**.

- **WV Breach Law (W. Va. Code § 46A-2A-101):**

The *unauthorized* disclosure or access of the Personal Information (PI) of anyone: **faculty, staff, parents, guardians and students**.

# FERPA

Disclosure means "to permit access to or the release, transfer, or other communication of **personally identifiable information** contained in education records to any party, by any means, including oral, written, or electronic means."  
34 CFR § 99.3

- **PII includes, but is not limited to:**

- The student's name
- The name of the student's parent or other family member
- The address of the student or student's family
- A personal identifier, such as the student's social security number or student number
- A list of personal characteristics that would make the student's identity easily traceable
- Any other information that would make the student's identity easily traceable.

All information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual.

[https://studentprivacy.ed.gov/ferpa#0.1\\_se34.1.99\\_130](https://studentprivacy.ed.gov/ferpa#0.1_se34.1.99_130)

# Consider some other identifiers.

Can these be used in to identify a Student?

Can these be used in combination to identify a student?

- Telephone numbers
- Vehicle identifiers
- E-mail addresses
- Web URLs and IP addresses
- Dates (except year)
- Names of relatives
- Geographic subdivisions (smaller than state)
- Full face photographs or images.
- Healthcare record numbers
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Any other unique number, code, or characteristic that can be linked to an individual

# WV Breach Code

## **Personal Information (PI) is defined as:**

- the first name or first initial and last name; linked to
- any one or more of the following data elements:
  - Social Security Number
  - Driver's license number or state identification card number issued in lieu of a driver's license
  - Financial account number, or credit, or debit card number in combination with any required security code, access code or password that would permit access to...financial accounts."
- when the data elements are neither encrypted nor redacted.

We've had a data privacy incident.  
Now what?

**Report!**



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



# Incident Report Portal



## **File an Incident Report (same location, two URLs)**

- State Privacy Office website > Incident Response page
  - <https://privacy.wv.gov/incidentresponse/Pages/default.aspx>
- WV Office of Technology website > Report Incident page
  - <https://apps.wv.gov/ot/ir/>

# Incident Report Information

## Contact Information

- Name
- County BOEs
- Office Phone
- Cell/Pager
- Email

## Incident Information

- Physical Address
- Date and Time of Incident
- Brief Summary - Include any steps taken so far to mitigate incident
- Impact of Incident – If known
  - Number of People
  - Types of PII exposed or compromised
  - Do not include actual PII
- Is the incident ongoing?



WVOT Online Computer Security and Privacy Incident Reporting System

Contact Information

\*Name:

\*Agency:

\*Office Phone:

Cell/Pager:

Email:

# Incident Report: Automatically filed with

- BRIM
  - Executive Director
  - Claims Department
  - State Privacy Office
- WV Office of Technology – Cyber Security Office

# BRIM: Roles and Next Steps

- Privacy staff will reply to sender that report was received
- Notify BRIM's BOE county contact regarding incident
- Technical assistance, including triage for determining next steps
- Risk management
  - Breach coach
  - Notification determination
  - Digital forensics expertise
  - Incident and notification assistance and PR

# BOE Staff: Roles and Next Steps

- Contain incident
  - Cyber - Breach Coach resources?
- Communication
  - Leadership
  - IT personnel
  - Activate Board's Incident Response Team
  - Law Enforcement – if theft is involved

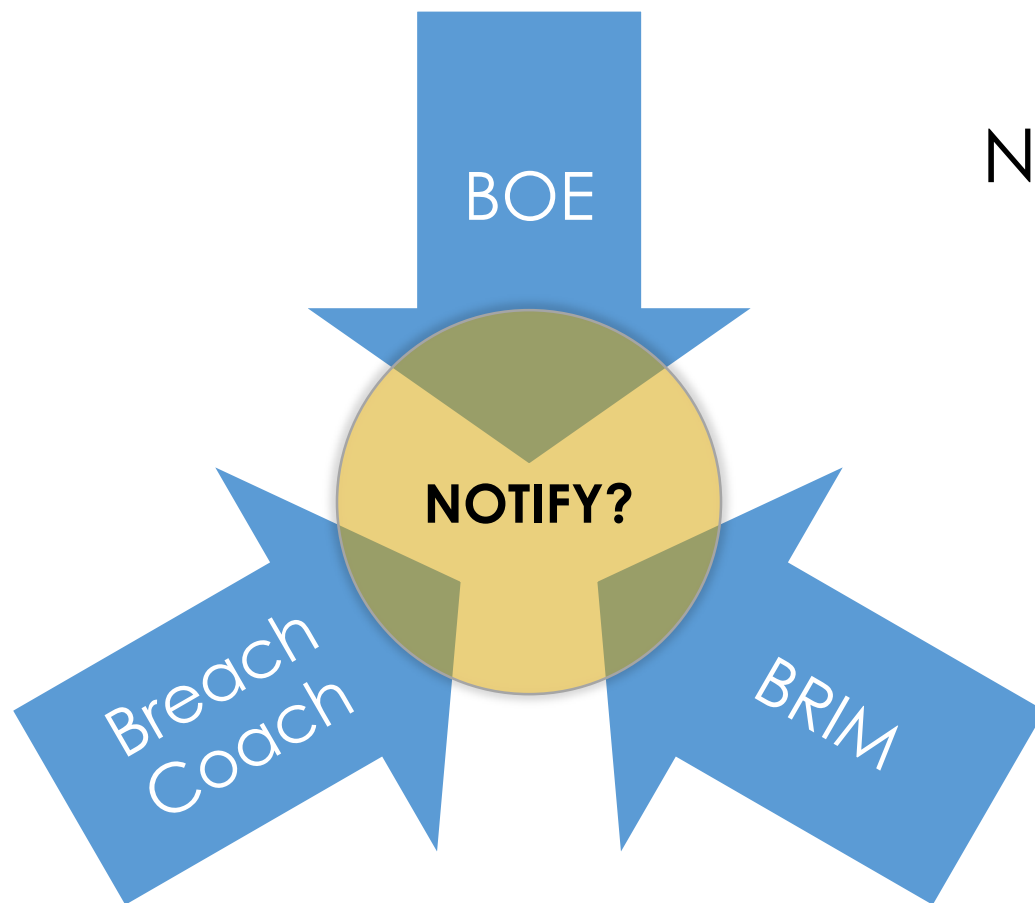
# BOE Staff: Roles, Next Steps and Tips

- Investigate Incident
  - Who, What, When, Where, How
  - Interview witnesses and/or affected parties
  - Determine affected individuals, *including **state** of residence*
  - Determine potential impact on systems and any other organizations
  - **Do a root cause analysis of systems and processes**
- Be aware of Special Rules – If Applicable
  - Payment Card Industry – Data Security Standards

# BOE Staff: Roles, Next Steps and Tips

- Mitigation
  - Return of documents and/or technology
  - Document deletion of data
  - Get signed affidavits of non-disclosure
  - ***Fix problems and processes***
- Document, document, document!
  - Investigation findings
  - Mitigation steps
  - Changes made

# Notification Determination



Notification of affected parties:

- Per WV State Breach Code;
- Other state's laws (if applicable); and,
- Determined in conjunction with the BOE, BRIM and the breach coach.



# RESOURCES





# Confidentiality Agreements with Staff

## Purpose

- Follow law and policy regarding confidential information (CI)
- No disclosure of CI for personal or non-work related reason
- Safeguard CI

## Resources

- WV Executive Branch Confidentiality Agreement, <https://privacy.wv.gov/SiteCollectionDocuments/Privacy%20Policies/1c%20Confidentiality%20Agreement%20Document.pdf>

# Privacy Policies

## Purpose

- Essential to the proper protection and management of personal information
- Needed to manage risk of data breach

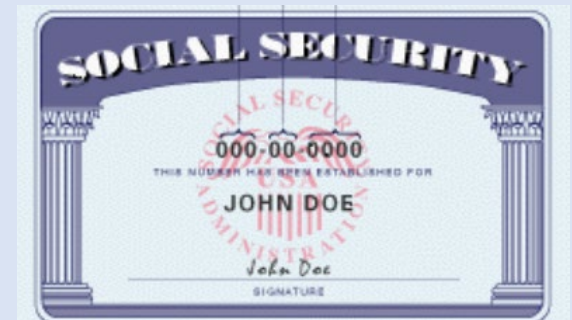
## Resources

- WV Executive Branch Privacy Policies and Procedures:  
<https://privacy.wv.gov/privacypolicies/Pages/default.aspx>
- eRisk Hub's Incident Response Plan Policy\*

# Privacy and Security Training Resources

- 150+ Privacy awareness tips: <https://privacy.wv.gov/tips/Pages/default.aspx>
- Security training resources: contact WV's CISO, Danielle Cox [https://technology.wv.gov/security/Pages/contact\\_information.aspx](https://technology.wv.gov/security/Pages/contact_information.aspx)

- eRisk Hub\*
  - Training Policy
  - Security & Privacy Awareness Training - video modules and quizzes



# Record Retention and Secure Disposal

- Retain personal information no longer than required
- County BOE Financial Record Retention Schedule:  
<https://wvde.us/wp-content/uploads/2018/02/Records-Retention-Schedule.pdf>
- WV Student Record Retention Schedule: WVBE Policy 4350.  
<http://apps.sos.wv.gov/adlaw/csr/readfile.aspx?DocId=29947&Format=PDF>



# Security Policies

## Security Overview

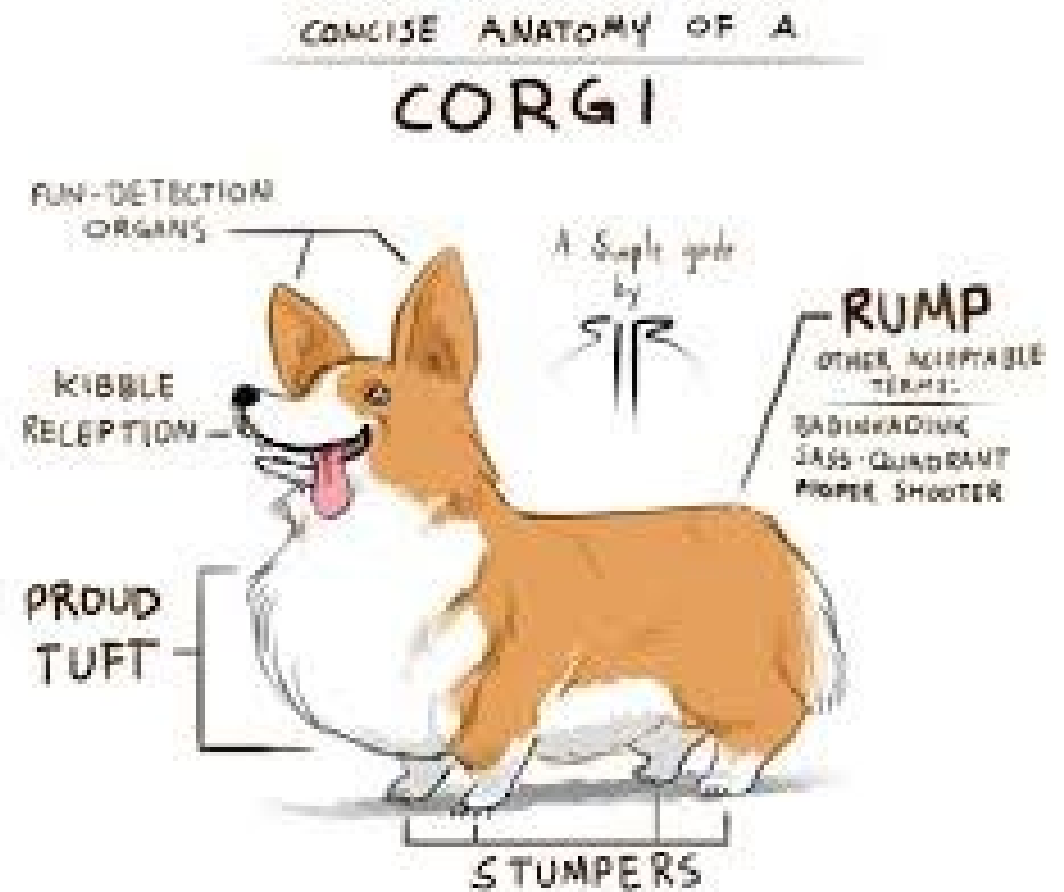
- Require information to be appropriately safeguarded to ensure confidentiality, integrity and availability
- Three domains
  - Administrative
  - Physical
  - Technical

## Resources

- WV Executive Branch Security Policies and Procedures:  
<https://technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx>
- eRisk Hub's Sample Security Policies\*

# Data and System Classification

- Policy to categorize information and information systems
- Accounts for risk
- Resources
  - WV Data Classification Policy: [https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1006\\_DataClassification\\_Mar2019.pdf](https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1006_DataClassification_Mar2019.pdf)
  - eRisk Hub\*: asset inventory with risk assessment



<http://corgis-everywhere.tumblr.com/post/45782366406>



# Access control policy

- Require strong authentication and audit account access and permissions
  - Complex passwords, biometrics, tokens
  - Audit account access
  - Remove old accounts and unnecessary privileges
- Resource: WV Executive Branch Account Management Policy:  
[https://technology.wv.gov/SiteCollectionDocuments/Policies%20Isued%20by%20the%20CTO/2019/PO1021\\_AccountManage\\_Mar2019.pdf](https://technology.wv.gov/SiteCollectionDocuments/Policies%20Isued%20by%20the%20CTO/2019/PO1021_AccountManage_Mar2019.pdf)

# Data Back-up

- Do you have a back-up policy and procedure to protect critical information systems and data?
- Do you annually verify that it is working?
- Resource: WV Executive Branch Policy:  
[https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013\\_DataBackup\\_Mar2019.pdf](https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)

# Legal Resources

- WV Department of Education:  
<https://wvde.state.wv.us/zoomwv/data-privacy.html>
- FERPA summary with links to resources and law:  
<https://privacy.wv.gov/SiteCollectionDocuments/Legal/2019%20Privacy%20Requirements%20-%20Final.pdf>

# eRiskHub

## To access the Gallagher eRiskHub:

1. Navigate to <https://eriskhub.com/gallagher>
2. Complete the new user registration at the bottom of the page. You pick your own user ID and password. The access code is: **447597**.
3. After registering, you can access the hub immediately using your newly created credentials in the member login box located in the top right of the page.

# Q & A

# Contact Information

## **Board of Risk and Insurance Management**

1124 Smith Street, Suite 4300

Charleston, WV 25301

Phone 304.766.2646

Toll Free 800.345.4669

FAX 304.558.6004

- Mary Jane Pickens, Director of BRIM – Ext. 57009 – [maryjane.pickens@wv.gov](mailto:maryjane.pickens@wv.gov)
- Melody Duke, Underwriting Manager – Ext. 57618 – [melody.a.duke@wv.gov](mailto:melody.a.duke@wv.gov)
- Ashley Summitt, Chief Privacy Officer – Ext. 57624 – [ashley.e.summitt@wv.gov](mailto:ashley.e.summitt@wv.gov)
- Lori Tarr, Assistant Chief Privacy Officer – Ext. 57616- [lori.l.tarr@wv.gov](mailto:lori.l.tarr@wv.gov)
- Sue Haga, Administrative Secretary (Privacy Office) – Ext. 57626 – [sue.c.haga@wv.gov](mailto:sue.c.haga@wv.gov)