WV BOARD OF RISK AND INSURANCE MANAGEMENT

Board of Education

Cyber Liability and Awareness

May 16, 2018

WVASBO Spring Conference

1

Agenda

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

2

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.

4

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.

5

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.

7

Overview of BRIM

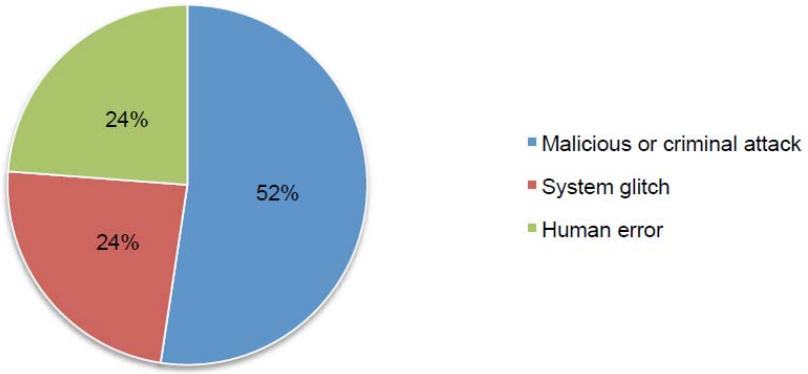
- BRIM has 24 full-time employees:
  - 5 Underwriting,
  - 6 Claims,
  - 4 Loss Control,
  - 4 Finance;
  - 2 Administration, and
  - 3 Privacy Office.

UNDERSTANDING THE BREACH THREAT

Root Causes of a Data Breach

Distribution of Benchmark Sample

Source: Ponemon Institute: 2017 Cost of Data Breach Study: United States

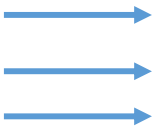


10

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/



Don't be fooled

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

System Glitches

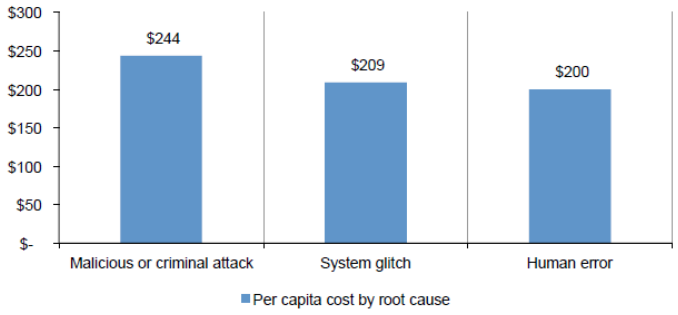
- Application errors
- Inadvertent data dumps
- Logic errors in data transfer
- Identity or authentication failures (wrongful access)
- Data recovery failures

- Source

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

Per Capita (Record) Breach Cost by Root Cause

Ponemon Institute: 2017 Cost of Data Breach Study: United States



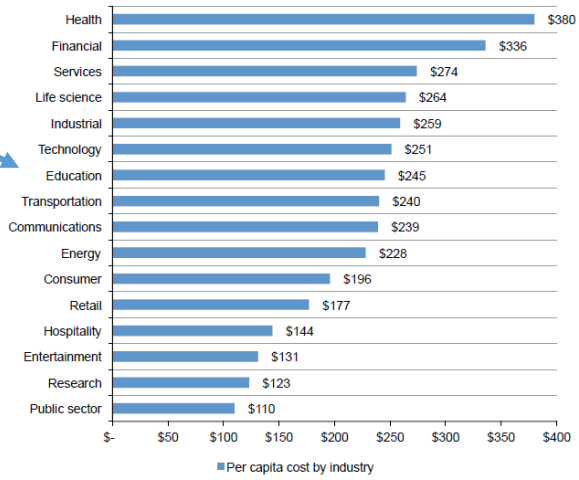
14

Per Capita (Record) Breach Cost by Industry

Ponemon Institute: 2017 Cost of Data Breach Study: **United States only**

Education sector: 7th highest of 16

- $245 per education record
- $225 per overall US median



Education Dive – Quotes Ponemon Study

Education Dive: Website that covers Education news

Cost of education data breaches averages $245 per record

Dive Brief:

- Average cost of US education industry rose to $245 per record lost
- $45 above worldwide average
- Two trends in K-12, Higher Ed increase cost
  - Increased use of mobile platforms
  - Compliance failures
- ***Delays in detection and containment contribute significantly to high cost for education***

Source: https://www.educationdive.com/news/cost-of-education-data-breaches-averages-245-per-record/447376/

16

Cyber Liability Policy

Insurer: AIG Specialty Insurance Company

17

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 90th day after a PR firm is hired in response to the Reputation Threat.

DATA PRIVACY INCIDENT RESPONSE

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-10):**

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

25

Defining Further

- **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.

26

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

Defining Further

WV Breach Law:

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 ..., when the data elements are neither encrypted nor redacted:

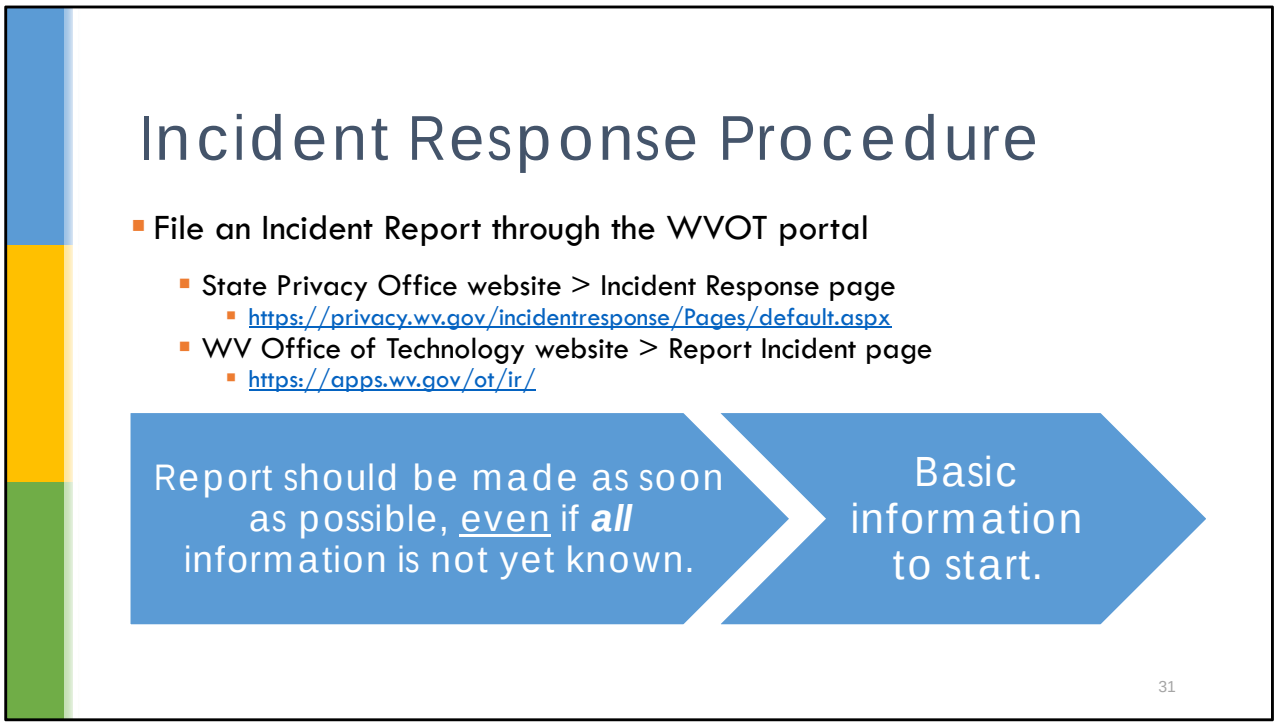
- Social Security Number
- Driver's license number or state identification card number issued in lieu of a driver's license
- Financial account number, or credit, or debit card number in combination with any required security code, access code or password that would permit access to...financial accounts."

Example Situation – Spear Phishing Email

- **Sent to:** You; Superintendent; Deputy Superintendent; Director of Support Services; and, the Executive Secretary
- **Subject:** Lawsuit Threat
- **Sent from:** Board's General Counsel (appears to)
- **Text:** States that the attached file contains more information about a lawsuit that may be filed against the County Board next week
- **Setting:** It's late in the day and one of the recipients downloads and opens the document
- **Problem:** It is a spoofed email. It goes undetected until the next day, when the recipient asks the General Counsel about the "corrupt" file attached to the email about the lawsuit
- **Outcome:** The system is now infected and the entire network is compromised

Now what? Without a process in place and prior training, valuable time can be lost in mitigating an incident. With training, it's known that the Incident Management Process needs to be activated. And there are tools to help. There is an Incident Response Checklist, that has room for notes. And there is a half page reference card that can be pinned on a bulletin board for quick reference.

Both of these are located on the Privacy Office's website, on the Incident Response tab under the link for the Incident Response Table-top Exercise Documents



The first step is to file the incident through what is called the Incident Report Portal. Here is the direct link and it can also be found on the State Privacy Office website on the Incident Response page.

Not only is this the first step in the process, but it should be made as soon as possible – even when all the information is not yet known.

>>>>>>>>>>

Incident Management Procedure

- **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?

32

There is some basic information that is needed to file the report. It asks for:
(1) Contact information (Name, agency, phone numbers and email) and
(2) Information about the incident itself.

You'll want to know where it occurred, when it occurred – including date and time (if known), and be able to provide a brief summary, including any steps taken so far to mitigate the incident.

Also, if it's known or can be estimated, provide information on the impact of the incident such as the number of people whose PII may be compromised, and the specific data types, such as name, address, Social Security Numbers, Date of Birth, etc.

But do NOT include any actual PII.

Finally, give your best understanding if this incident ongoing? By that we mean, is the information still vulnerable?

Filing the Incident Report automatically notifies:

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

33

BRIM: Roles and Next Steps

- Privacy staff will reply to sender with receipt of report message
- Notify BRIM BOE contact regarding incident
- Technical assistance, including triage for determining next steps
- Risk management
  - Breach coach
  - Notification determination
  - Incident and notification assistance, forensics and PR

BOE Staff: Roles, Next Steps and Tips

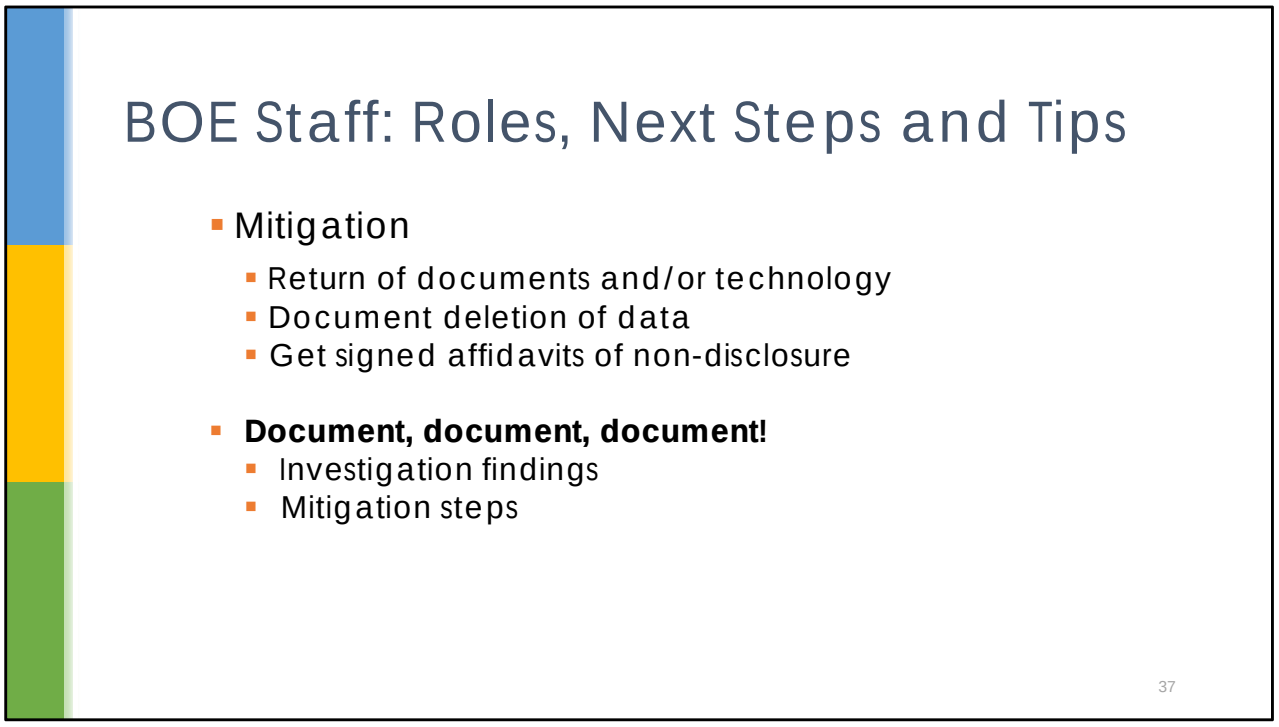
- Contain incident
  - Cyber - Breach Coach resources?
- Notify
  - Leadership
  - IT personnel
  - Activate Board's Incident Response Team
  - Law Enforcement – if theft is involved

After the initial Incident Report is filed, there will likely need to be more information gathered by the DPO, especially if the first report was filed by someone else. On the checklist, step two provides a list of questions to get answers to, if not already know. There are the what, when, where questions, plus systems questions. Was the data encrypted, what systems were involved, what. Has the loss of data been stopped. As much as possible the DPO should get up to speed with what is or can be known. And, if it's an incident involving information systems, it's very likely that the DPO will be working closely with OT to contain the incident.

The DPO is responsible for notifying other stakeholders as appropriate. In our example incident, the spear phishing attack involved the leadership, so they may already be aware. However, the DPO should be prepared to keep leadership apprised as more is learned. And depending on where in the Department the incident occurred leadership might not be aware of it. This is part of the responsibility of the DPO to keep leadership informed, and make other proper notifications: IT connections, activate the Department's Incident Response Team if they have one, and contact law enforcement if theft is involved. These are steps are 3 – 6 on the checklist.

Some of you maybe noticing this process may not be perfectly linear. How you manage an incident; What steps you'll have to take and retake – will depend on the complexity and impact of the incident. If it's a complicated incident there may be more investigation called for. There may be witnesses or affected parties to interview. It may take a while to determine who the affected parties are be it individuals or other organizations. It may be clear that more training should occur and a root cause analysis be completed of what went wrong so policies and procedures can be put into place to keep it from happening again. Step 7 on the checklist has a list of questions. This is not everything or it may not be relevant. This list is a starting point. Whatever can be known to reduce the impact of the current incident or to stop a future incident is where the investigation should take you.

>>>>>>>>>>>>>>>>>>>>>>



Step 8 on the checklist relates to recovery of data elements. Sometimes, an incident is as simple as a document with PII mailed to the wrong person. In that case it may be as simple as getting the document returned. And it may involve getting affidavits signed that the data viewed will not be disclosed.

Step 9 & 10 of the checklist relates to data that have special rules. If the incident is related to medical information, credit cards or taxes there are special rules and standards involved that call for specific actions.

>>>>>>>>>>>>>>>

RESOURCES

Resources for many best practices

https://www.surreyschools.ca/sites/7V5JQUO4HC/Pages/default.aspx

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

40

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*

41

Privacy and Security Training Resources

- 150+ Privacy awareness tips: https://privacy.wv.gov/tips/Pages/default.aspx
- Security training resources: contact WV's CISO, Joshua Spence at 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

43

WVBE Policy 4350 addresses records retention issue for student records in a couple of places but most specifically in §126-94-12 (Maintenance and Destruction of Education Records).

§126-94-12. Maintenance and Destruction of Education Records.

12.1. An educational agency or institution is not precluded from destroying education records, subject to the following exceptions:

12.1.a. The agency or institution may not destroy any education records if there is an outstanding request to inspect and review them under Section 126-94-9;

12.1.b. Explanations placed in the education record under Section 126-94-14 shall be maintained as long as the record or the contested portion is maintained;

12.1.c. The record of access required under Section 126-94-20 shall be maintained for as long as the education record to which it

pertains is maintained; and

12.1.d. For records collected for students with exceptionalities under Policy 2419: (a) the public agency shall inform parents when personally identifiable information collected, maintained, or used is no longer needed to provide educational services to the child; (b) the information must be destroyed at the request of the parents; (c) however, a permanent record of a student's name, address, and phone number, his or her grades, attendance record, classes attended, grade level completed, and year completed may be maintained without time limitation.

12.2. The following guidelines and requirements apply to the length of time and special consideration for maintaining student records:

12.2.a. Directory information may be maintained in perpetuity;

12.2.b. Academic grades and attendance records may be maintained in perpetuity;

12.2.c. Records to verify implementation of federally funded programs and services and to demonstrate compliance with program requirements must be maintained for five years after the activity is completed;

12.2.d. Other personally identifiable data which is no longer needed to provide education services may be destroyed;

12.2.e. Parents and eligible students must be informed through public notice of any timelines established by the educational agency or institution for maintenance and destruction of student records; and

12.2.f. Files must be maintained in a secured location. Inclusive in securing files, electronic files must be protected through the use of individual user identification and/or passwords. When user identification and/or passwords have been established, an individual is permitted to use only his or her designated identification and password to gain access to education records.

Security Policies

Security Overview

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

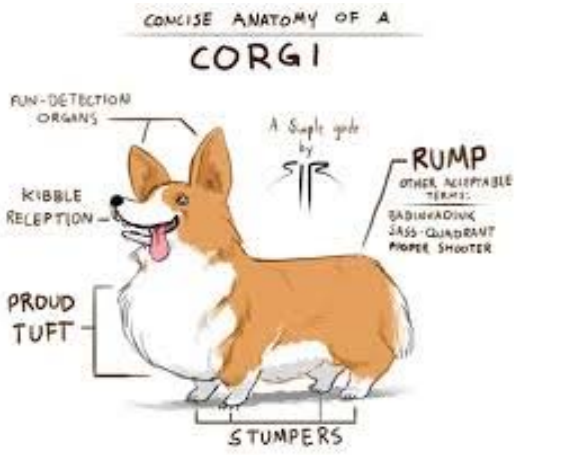
Resources

- 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*

44

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/2017/PO1006_DataClassification_Sept2017.pdf
  - eRisk Hub*: asset inventory with risk assessment



Encryption

Encryption Benefits

- Encryption makes data unknowable and unreadable
- Possible legal safe harbor
- Encrypt all BOE-owned laptops, tablets and smartphones

https://www.howtogeek.com/234642/what-is-encryption-and-why-are-people-afraid-of-it/

Resources

- Encryption for laptops: https://www.ed.ac.uk/infosec/how-to-protect/encrypting/encrypting-computer-laptop
- Encryption for smartphones and tablets:
  - https://www.pcworld.com/article/258974/tablet_encryption_101.html
  - https://www.ed.ac.uk/infosec/how-to-protect/encrypting/encrypting-smartphones-and-tablet-devices

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%20Issued%20by%20the%20CTO/2017/PO1021_AccountManage_Sept2017.pdf

47

Vulnerability scanning of systems

Scanning

- At least quarterly
- Validate that vulnerabilities are addressed in accordance with a risk management methodology

Resources

- WV Office of Technology Vulnerability Scanning Service: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2017/VulnerabilityScanningAuthorizationFormv2.pdf
- Free vulnerability scanners: https://www.networkworld.com/article/2176429/security/security-6-free-network-vulnerability-scanners.html

48

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/2017/PO1013_DataBackup_Sept2017.pdf

Legal Resources

- FindLaw: https://statelaws.findlaw.com/west-virginia-law/west-virginia-privacy-of-school-records-laws.html
- FERPA summary with links to resources and law: https://privacy.wv.gov/SiteCollectionDocuments/Legal/2017%20Privacy%20Requirements.pdf

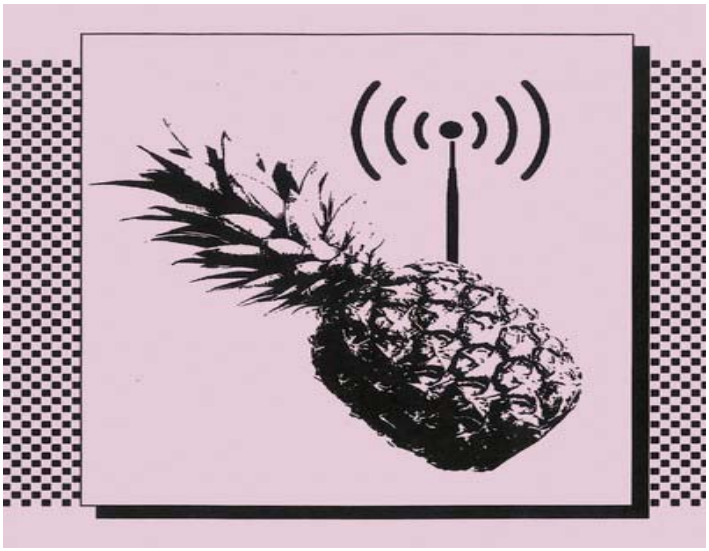
50

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 **08167.**
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.

51



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 or BRIM – Ext. 57009 – maryjane.pickens@wv.gov
- Melody Duke, Underwriting Manager – Ext. 57618 – melody.a.duke@wv.gov
- Sallie Milam, Chief Privacy Officer – Ext. 57624 – sallie.h.milam@wv.gov
- Lori Tarr, Assistant Chief Privacy Officer – Ext. 57616- lori.l.tarr@wv.gov
- Sue Haga, Administrative Secretary (Privacy Office) – Ext. 57626 – sue.c.haga@wv.gov