WISCONSIN ASSOCIATION OF SCHOOL BOARDS, INC.
122 W. WASHINGTON AVENUE, MADISON, WI 53703
PHONE: 608-257-2622 · FAX: 608-257-8386

Developing a Cybersecurity Incident Response Plan

Topic Objectives:

1. Why should a district have a Cybersecurity Incident Response Plan (CIRP)?
2. What tools and templates are available to help districts develop a CIIRP?

Districts prepare and train for managing tangible intruders, fires and student altercations. Why? Because faculty and staff need to know *ahead of time* how to respond when these events occur. Likewise, since reports of IT incidents and actual breaches are now fairly common, it makes sense to prepare district staff for managing this possibility as well.

A cybersecurity incident is anything prompting district personnel to think the district's IT system has been breached or confidential information has been unknowingly released. A cybersecurity breach is when the district's IT system has actually been breached (hacked) by an unauthorized person, entity or program (virus, malware). The impact of a breach is too expansive to describe, though can, for example, result in the release of personally identifiable information ("PII"), stolen payroll, or district data being held for ransom. For the purposes of this article, breaches are considered cybersecurity incidents.

1. <u>Why should a district have a CIRP?</u>

   Though too numerous to list, two significant reasons should suffice:

   A. Decrease Your Anxiety

      Think worst case scenario; for example, the database holding your staff's 941 information is accidentally attached and released via email to an outsider posing as an auditor.

      - What is the first thing you do?
      - What is the second thing you do?
      - Who executes steps #1 and #2?
      - Who do you notify?
      - Are you required to notify anyone? When?
      - What do you say to your staff?
      - What do you say to the press?

      Get the picture? Be selfish, have an CIRP so you're not running down the hall with hair on fire deciding what to do when a cybersecurity incident occurs.

B. Decrease Your Response Expenses

According to the Ponemon Institute's *2018 Cost of a Data Breach Study: Global Overview*, on average, an educational institution spends $166 per record to respond to a breach. One record = the release of one staff member's name, date of birth and social security number.

This same study indicated having an CIRP decreases the per record response cost by almost 10%! Even if you carry breach response insurance, it makes sense to have a CIRP.

2. What tools and templates are available to help districts develop a CIRP?

There's no need to reinvent the wheel. CIRP templates are available from many sources such as:

- WASB endorsed insurance agencies Arthur J. Gallagher, M3 and TRICOR (https://wasb.org/wasb-insurance-plan/);
- Your cyber insurance company. Many of them offer access to NetDiligence (cyber risk management services) at no additional cost;
- Your peers; and
- The internet. For example, *https://www.exabeam.com/incident-response/incident-response-plan/.

**The WASB Insurance Plan does not endorse this company or its offerings.*

Conclusion: There's no reason to not have a CIRP for your district. Administrators and IT personnel alike can benefit from using templates and peer input to develop (but hopefully never have to activate) a CIRP. Review several different templates before deciding on the form most appropriate for your district. A CIRP will save you time, money and sleep!