CENTER FOR DEMOCRACY & TECHNOLOGY

CYBERINSURANCE AND CYBERSECURITY IN SCHOOLS

PRIORITIZING IMPACTFUL PRACTICES

August 2021

What is Cyberinsurance?

As schools continue to face cyberattacks, cyberinsurance aims to offer schools a way to mitigate the costs and impacts of these attacks. For instance, in the event of a cyberattack, an insurance plan *may* provide:

- **Remediation expenses**, such as the cost of improving the system to eliminate the vulnerability that caused the breach;
- **Financial liability expenses**, like repaying funds inadvertently transferred to attackers, or covering the cost of credit monitoring for those who may have had data exposed by the attack;
- **Legal expenses** and, depending on the circumstances, civil damages;
- **Notification expenses** like letters to inform affected individuals about the incident; and
- Access to services such as **computer forensic technicians** to help determine how the system was attacked and to prevent future incidents.

As an additional benefit, schools can use insurance plans and questionnaires as a way to focus their *own* cybersecurity improvement efforts on the most impactful practices.

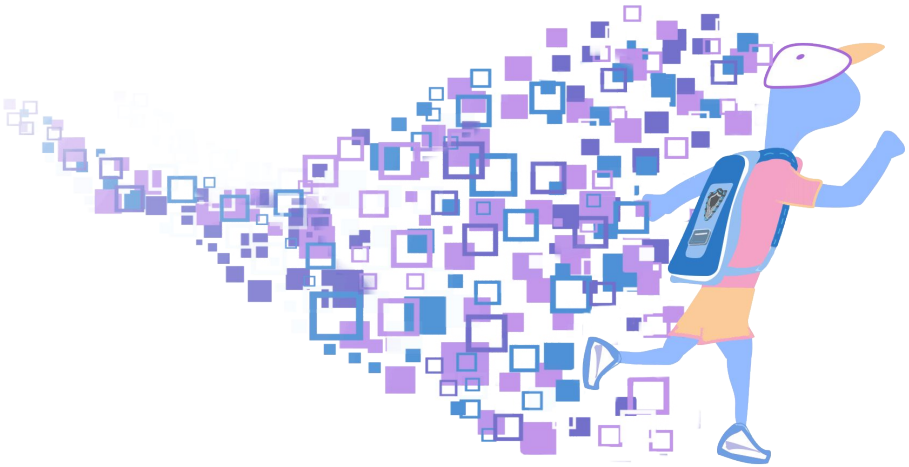
Using Cyberinsurance Plans for Cybersecurity

Insurance companies want to limit the likelihood they will need to pay out on a policy.

Consequently, they screen organizations' cybersecurity infrastructure and practices, focusing on those practices that are most likely to determine whether or not a school is vulnerable to a cyberattack based on insurance companies' research and experience with a variety of claims.

Schools can use an insurance company's questions to help evaluate their own security practices, regardless of whether they ultimately purchase a given insurance policy.

Cybersecurity Improvements



Cybersecurity Best Practices - Part 1

To focus cybersecurity improvements on some of the most impactful areas based on insurance company research, consider some of the most commonly asked questions from several policy applications:

- **Does the school have a designated person or office who is responsible for information security?**
  - Having a designated person in charge of cybersecurity can help ensure that cybersecurity is not lost amongst competing priorities within the school.
- **What training is provided to employees on security issues and procedures?**
  - Most data breaches are the result of human errors, meaning that training employees on security practices is a critical element of avoiding data breaches and cyberattacks, as well as minimizing the consequences should an attack occur.
- **What data protection and security controls (e.g., firewalls) does the school employ?**
  - These controls are designed to keep malicious attackers off of school computers and systems, which can help avoid cyber attacks.

Cybersecurity Best Practices - Part 2

Other common questions from insurance policies include:

- **Does the school maintain back-up copies of data and systems?**
  - Backups are valuable in ransomware attacks, because a school can restore its data and system from its own backups, rather than having to choose between paying the ransom or losing the data.
- **Does the school maintain up-to-date privacy and security policies?**
  - Clear policies can help employees understand how to keep data and systems safe (though these policies should be coupled with training for those who use the systems).
- **Does the school maintain sensitive data like credit/debit card information, social security numbers, or medical information?**
  - These types of data can be particularly damaging if exposed. Consequently, schools should focus data protection efforts, like encrypting data at rest and deleting unneeded data, on these types of data to avoid particularly damaging breaches.

Cybersecurity Best Practices - Part 3

There are a number of other important questions that come up in a number of policy applications:

- **Has the school implemented security features like multi-factor authentication and access control procedures?**
  - These procedures can help to keep accounts and data secure, and minimize the potential damage in the event that an account is compromised by an attacker.
- **Does the school maintain a data destruction and retention policy?**
  - Maintaining and following such policies limits the amount of data stored by a school, thus limiting the impact of a breach.
- **Does the school have an incident response plan for responding to a cyberattack?**
  - Having a plan in place ahead of time can ensure that employees are able to take effective action in the event of an incident, rather than losing time trying to figure out what to do.

CYBERSECURITY RESOURCES

Cyberinsurance and Cybersecurity Resources

- **Phishing detection tips:** The Freedom of the Press Foundation offers a primer about detecting and managing phishing emails: https://freedom.press/training/email-security-tips/
- **Multi-factor authentication:** CDT's primer on multi-factor authentication can help schools take advantage of this technology: https://cdt.org/insights/election-cybersecurity-101-field-guide-two-factor-authentication/
- **Data deletion and retention:** CDT's guide on data deletion in education can help schools limit the risks of maintaining unnecessary data: https://cdt.org/insights/report-balancing-the-scale-of-student-data-deletion-and-retention-in-education/
- **Ransomware and cybersecurity:** The Cybersecurity and Infrastructure Security Agency has resources for helping K-12 institutions manage ransomware, much of which focuses on improving their overall security: https://www.cisa.gov/stopransomware/k-12-resources

CDT'S VISION

PUTTING DEMOCRACY AND INDIVIDUAL RIGHTS AT THE CENTER OF THE DIGITAL REVOLUTION

CDT's Equity in Civic Technology Project

- *Provide **balanced advocacy** that promotes the responsible use of data and technology while protecting the privacy and civil rights of individuals.*
- *Create **solutions-oriented policy resources** that are grounded in the problems that currently confront policymakers, practitioners, and technology providers who work with them.*
- *Offer **technical guidance** that can be adapted and implemented by policymakers, practitioners, and the technology providers who support them.*

Contact Us

Equity in Civic Technology Project
Center for Democracy & Technology
CivicTech@cdt.org