Cyber Coverage and Risk Management Strategies for Vermont K-12 Public Schools

multi-line
Vermont School Boards Insurance Trust

Presented 10/19 and 10/20 2021
Ken Canning, Multi-Line Program Manager
Dave Pickel, Manager of Risk Services
Ben Provost, Risk Management Consultant

The Cyber Insurance Market

- Top 10 cyber insurance carriers (controls about 70 - 75% of the marketplace) all report an overwhelming increase in ransomware claims
  - No industry class was spared
  - Public Entity was the most successfully targeted sector in terms of penetration by the attackers and frequency
    - Amongst the least prepared due to older software/computer equipment, lack of training, low IT security budgets
- The Public Entity sector is now being viewed very closely by Insurance Company management, and continuing to tighten
    - Especially for large public entities and JPAs/Pools/Public Entities with Protected Health Information, carriers are worried about the vast number of members with the same ransomware exposure under the same policy
    - Many markets no longer writing **new** Public Entity cyber

How VSBIT Can Help

- Cyber risk management is the process of identifying, analyzing, evaluating and addressing your organization's cyber security threats. The first part of any cyber risk management program is a cyber risk assessment.
- Cyber loss control is a risk management technique that seeks to reduce the possibility that a loss will occur and reduce the severity of those that do occur. A loss control program should help members reduce claims, and school risk pools like VSBIT reduce losses through safety and risk management information and services.
- Cyber risk transfer is another risk management technique where you transfer the financial consequences of the risk to another party. One way to do this by purchasing insurance coverage, which VSBIT does on your behalf. Another method is to transfer the risk to a third party via a contract, otherwise known as contractual risk transfer.

Cyber Liability – Limits

- Aggregate Limit – All Coverages and All Members Combined: $10,000,000
- Cyber Extortion Sublimit per Member: $100,000
- E-Discovery Consultant Services, Third Party Event $25,000
- Criminal Reward Coverage: $50,000
- Deductible Each Coverage: $25,000
- Network Interruption Waiting Hours Period: 12 Hours

Cyber Liability – Coverages Explained

- Security Failure
  Privacy Event
  Event Management
  Cyber Extortion
  Network Interruption
  Media Coverage
  A Security Failure is a failure or violation of the security of a Computer System including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack, or receipt or transmission of a malicious code; physical theft of hardware controlled by you (or components thereof) on which electronic data is stored from a premises occupied and controlled by you; or failure to disclose an event referenced above in violation of any Security Breach Notice Law.
  - Security Failure includes any such failure or violation, resulting from the theft of a password or access code from your premises, the Computer System, or an officer, director or employee by non-electronic means in direct violation of your specific written security policies or procedures.
- A Privacy Event is any failure to protect Confidential Information (whether by phishing or other social engineering technique or otherwise) including, without limitation, that which results in an identity theft or other wrongful emulation of the identity of an individual or corporation; failure to disclose an event referenced above in violation of any Security Breach Notice Law; or violation of any federal, state, foreign or local privacy statute alleged in connection with a Claim for compensatory damages, judgments, settlements, pre-judgment and post-judgment interest from above.
- Event Management includes the expense to conduct an investigation (including forensic investigation) to determine the cause of the Security Failure or Privacy Event; for a public relations firm, crisis management firm or law firm to advise you on minimizing the harm and restore public confidence; for any other approved services; to restore, recreate or recollect Electronic Data; or to determine whether Electronic Data can or cannot be restored, recollected or recreated.
- Privacy Event Expenses is the reasonable and necessary costs incurred to notify Affected Persons of such Privacy Event and advise of any available remedy in connection with such Privacy Event, including, without limitation, those expenses and costs for printing and mailing of materials; for identity theft call center assistance, identity restoration services, identity monitoring and victim cost reimbursement insurance provided to Affected Persons.
- A privacy threat means any threat or connected series of threats to unlawfully use or publicly disclose confidential information misappropriated from an insured for the purpose of demanding money, securities or other tangible or intangible property of value from an insured
- A security threat means 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 an insured

Minimum System Recommendations

- Multi-factor authentication – 100% implemented for:
  - Remote access
  - Laptops
  - Privileged access
- Well managed end point detection
- Well managed RDP connections
- Back Ups
  - 1 working copy, 1 offsite, disconnected not working, 1 onsite disconnected not working
  - Tested at least twice a year
  - Ability to bring up within 24-72 hours – less time for critical operations (4 hours)
  - Protected with antivirus or monitored on a continuous basis
  - Encryption
- Planning and Training
  - Incident Response Plan
  - Business Continuity Plan
  - Social Engineering Training
  - Phishing Training
  - Training of account team staff on fraudulent transactions
  - General cyber security training
- Reasonable patching schedule/plan
- Plan or adequate measures in place to protect end of life software

Cyber Data Collection

- Data collected to assess overall risk
- Collected from 46 SU/SDs in Vermont
- Some topics include:
  - Phishing mitigation
  - Web/Email Filtering
  - MFA
  - IT Policies and Procedures
  - Management of Antivirus/Security Tools
  - Admin/Access Control
  - Patching
  - Network/Server Management

Loss Control Strategies and Services

- **Platform to allow school IT professionals to implement periodic security awareness training to all staff and students**
- **Custom simulated phishing attacks and the ability to monitor and keep track of the success rate – goal is below 15%.**
- **Ransomware Exercises**
- **Multi-Factor Authentication**
- Web/email filtering
- Security tools/antivirus
- Admin/Access Control
- Patching
- Vulnerability scanning
- Backup capabilities/strategy
- Disaster Recovery Plans/Policies/Procedures
- Working with a third party administrator

How we Start

- Look at your SU/SD's data to assess needs:
  1. What data do you need to protect
  2. What do you have for storage needs
  3. Hardware and software
  4. Employee training (human firewall)
  5. MFA

QUESTIONS

Ken Canning, Multi-Line Program Manager; kenc@vsbit.org
Dave Pickel, Manager of Risk Services; davidp@vsbit.org
Ben Provost, Risk Management Consultant; ben@vsbit.org