Cyber Liability Insurance 101—Memo

Welcome to a quick overview of the information provided by NASPO in the "Cyber Liability 101" research brief. Cybersecurity is a top priority for NASPO and for more detail and explanation on this emerging issue, please check out the full brief by clicking here.

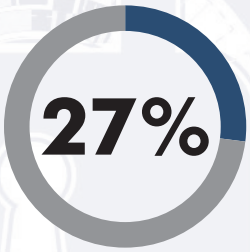
Cybersecurity by the Numbers

34,222,763
records compromised

In 2015 - **63 breaches** of government and military databases with **34,222,763 records compromised**

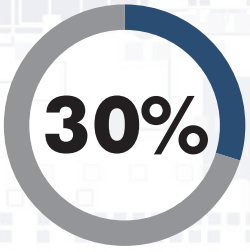
Average total cost of data breach in 2016 is **$4 million** *or* **$158 per lost/stolen record**

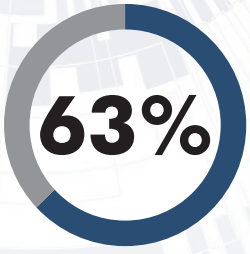
$4 MILLION
$158 per record



27% of states have established and funded state-level cybersecurity programs and framework for enterprise management.

30% of phishing messages are *opened by the target*, and **12%** go on to *click on the malicious attachment*.





63% of confirmed data breaches involved *weak, default, or stolen passwords*.

Common Cyber Liability Coverage Components

- **DATA BREACH AND PRIVACY CRISIS MANAGEMENT:**

  The investigation, the remediation, data subject notification, call management, and credit checking and monitoring

- **BREACH RESPONSE COVERAGE:**

  Legal consultation with breach response experts, forensic investigation expenses, data restoration or replacement expenses, public relations consultant expenses, notifying affected parties, and offering credit monitoring and repair

- **BUSINESS INTERRUPTION COVERAGE:**

  Business loss experienced during and immediately following a data breach

- **FIDUCIARY LIABILITY COVERAGE:**

  Penalties for violation of the law, prompt notice of the breach

- **CYBER EXTORTION/ RANSOMWARE COVERAGE:**

  Ransom/extortion demand, a consultant or expert to help negotiate with the hackers, and/or an expert to help block the attempted intrusion and reinforce the security

- **MEDIA LIABILITY COVERAGE:**

  Defense costs and liability arising out of claims alleging libel, slander, and/or infringement of intellectual property

- **PROFESSIONAL LIABILITY COVERAGE:**

  Defense costs and liability arising out of claims that allege negligence in providing a professional service such as a consultant, advertising agency, technology developer, and/or service provider

Five Suggestions for Prevention

1) INVEST IN PROPER CYBERSECURITY

- The importance of having the right cybersecurity software, encryption devices, and firewalls cannot be overstated.
- Update software regularly; educate staff about why that is important.

2) EDUCATE STAFF ABOUT PHISHING

- Educate staff with about what phishing messages look like.
- Prevent phishing by using strong email filters, segmenting your networks from one another, and requiring authentication when logging onto the network.

3) EMPHASIZE PASSWORD AND AUTHENTICATION SECURITY

- Choose a strong password and change it every 30 days.
- Limit access to hard and electronic data by staff, vendors, or service providers, based on their job or task requirements and duties.

4) CREATE A "SECURITY AWARENESS CULTURE"

- Empower staff, vendors, and service providers to be on guard for cyber attacks.
- Let staff know that the firewall will not always protect them.
- Create an environment where everyone feels comfortable asking for help or advice before making a questionable move on the network.

5) KNOW THE CYBER BREACH RESPONSE PLAN

- Staff should know to immediately document any breaches they become aware of, noting the date, time, and duration (if known) of the alleged breach.
- Educate everyone on whom to contact in the event of a data breach, and establish a method for reporting questionable activity or suspected breaches.
- Conduct training on your state or office's cyber breach response plan with staff at least once a year to emphasize the importance of such measures.
- Work with your state's CIO and CISO to educate everyone on your state's cyber liability policies and incident or breach response plans.