

CONSUMER ALERT

DAVE JONES, INSURANCE COMMISSIONER



www.insurance.ca.gov 1-800-927-4357

Cybersecurity risk management alert for consumers and businesses

Every two seconds someone is the victim of identity theft. Consumers need to be cautious and take action to protect themselves against identity theft and cybercrime. Businesses are also at risk, as we've seen with high-profile data breaches of large and small companies.

There are basic steps you can take to secure your information and data.

- Be alert to impersonators by being careful about who you trust online.
- Safely dispose of personal information by shredding documents using a cross-cut shredder.
- Use strict privacy settings on your computer, devices and browsers.
- Keep passwords private and complex.
- Be careful when sharing personal information on social media.
- Be cautious of what you download from the Internet.
- If your social security number is requested by a vendor, ask why it's needed and how it will be used and protected.
- Consider *identity theft insurance*.



What is identity theft insurance?

Some homeowners' or auto policies now offer identity theft protection, which includes access to credit monitoring and repair services in the event of a breach. In addition to homeowners policies, it's possible to find identity theft protection in a renter's policy, or an endorsement to a homeowners' or renter's policy. Note that this coverage only refunds the costs associated with restoring your identity. Restoring other losses would depend on the coverage policies of your credit card company and bank.

A growing area of concern in identity theft is stealing healthcare insurance. To combat this trend, doctors' offices and hospitals are increasingly using photo identification to make sure the person seeking treatment is actually the insured. In the world of electronic medical records, if someone uses your identity to seek treatment, their health conditions, medication allergies, and treatments could become part of your medical record, or be substituted for your record, creating a potentially dangerous situation when you need treatment—especially in an emergency when you may be unable to speak for yourself.

Your insurance agent may be able to help provide more information about assessing your risks and whether additional coverage is needed on home or auto policies.

CONSUMER ALERT

DAVE JONES, INSURANCE COMMISSIONER



www.insurance.ca.gov 1-800-927-4357

There are steps owners and employees can take to help secure your business:

- Start by conducting a security and risk self-assessment. Determine what to protect, what protection exists and where the gaps exist. This includes developing a plan to protect property and data, operational information, and client data. After conducting the self-assessment, it is important to identify the tools needed to protect this information.
- Implement sound cybersecurity procedures and training for employees. Educate employees on smart use of social media, spotting suspicious emails, and avoiding public WiFi networks when using a company device.
- Developing procedures and identifying threats is important, but business owners must also understand their vulnerabilities. They might consider testing such as an internal phishing campaign against employees to identify risky online behavior.
- Always back up important business systems and data. Implement settings encouraging regular password changes, restrictions on the websites employees can access, and deploy strong security software.
- If the small business has a disaster recovery plan, consider *cyber insurance* as part of it. If the company does not have such a plan, consider creating one.

What is cyber insurance?

Cyber insurance provides coverage for compromised security or privacy breaches at work. It is designed to mitigate risk exposure by offsetting costs of recovery following a cybersecurity breach. Cyber insurance typically covers expenses related to first parties as well as claims by third parties. [CIO Magazine](#) discusses the common reimbursable expenses: investigation, business losses, privacy and notification, lawsuits and extortion.

According to [PwC](#), about one-third of U.S. companies currently purchase some type of cyber insurance and the total value of premiums is forecasted to reach \$7.5 billion by 2020. Despite high profile data breaches of large companies, small companies are also targets for hackers as they possess sensitive information but typically have less security than larger companies. [Symantec](#) found that in 2015 small businesses with less than 250 employees were targeted in over 30 percent of phishing attacks and 43 percent of all cyber attacks.

Costs of a breach vs. cost of cyber insurance

[The Centre for Strategic and International Studies](#) estimated annual costs to the global economy from cyber-crime was between \$375 billion and \$575 billion. The average cost of a data breach incident to large companies is over \$3 million.

An example of a costly breach is the 2011 PlayStation hacker breach that resulted in an almost \$171 million loss to Sony that could have been vastly reduced if the company had thought to invest in cyber insurance coverage.

Business cybersecurity policies tend to be highly customized and therefore, costly. Each organization has to decide if they can risk that amount of money, or if cyber insurance is necessary to defray the costs for what very well may occur. Cyber insurance coverage and premiums are based on an organization's industry, type of services provided, data risks and exposures, security posture, policies and annual gross revenue.