NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

AUGUST 16, 2019

What's trending on NP Privacy Partner

What you need to know about the New York SHIELD Act and how overly vulnerable construction companies can protect themselves against cyberattacks. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

The New York SHIELD Act — What You Need to Know

At the end of July, New York Governor Andrew Cuomo signed into law the Stop Hack and Improve Electronic Data Security Act (SHIELD Act). The SHIELD Act amends and expands New York's current data breach notification law, which may affect persons or companies that do not even conduct business in New York. Here's what you need to know ahead of the March 21, 2020, effective date:

Who must comply?

Any person or business that owns or licenses computerized data, which includes private information of New York residents, must comply with the SHIELD Act, regardless of whether that person or business even conducts business in New York.

An expanded definition of "private information."

New York's data breach notification law has always varied from similar laws in other states in that it includes definitions for both "personal information" and "private information." Under the SHIELD Act, "personal information" remains "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." "Private information" captures the information that, if breached, could trigger a notification requirement. The SHIELD Act expands "private information" to include:

- Personal information consisting of any information in combination with one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:
    - Social security number,

    - Driver's license number or non-driver identification card number,
    - Financial account numbers with required security codes or access codes, or
    - Biometric information.
- A user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Access alone constitutes a "breach of the security of the system."

The SHIELD Act broadens the phrase "breach of the security of the system," which consequently broadens the circumstances under which notification is required. Notably, the SHIELD Act includes in the definition of "breach of the security of the system" incidents that involve "access" to private information, regardless of whether the access led to "acquisition" of the information. Under the original New York data breach notification law, data must have been acquired to constitute a breach. The SHIELD Act keeps intact certain exceptions to the definition of "breach" including the "good faith employee" exception and provides factors for determining whether there has been unauthorized access to private information.

Notably, companies that are already subject to the data breach notification requirements under certain applicable state or federal laws, including HIPAA, GLBA, and the NYS DFS Regulation 500, are not required to further notify affected individuals. However, notifications to the New York Attorney General, the New York State Department of Consumer Protection, and the New York State Police are still required.

A risk assessment is now permitted.

The SHIELD Act does not require notification of the breach if "exposure of private information" was an "inadvertent disclosure and the individual or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials." This risk assessment should be memorialized in writing.

Reasonable data security requirements are imposed.

The SHIELD Act also imposes data security requirements on any person or business that owns or licenses computerized data that includes private information of New York residents. These security requirements must be designed to protect the security, confidentiality, and integrity of the private information. The SHIELD Act provides examples of practices that are considered reasonable, including: (i) risk assessments, (ii) employee training, (iii) due diligence for vendor selection, and (iv) data retention and disposal policies.

Companies subject to HIPAA and the GLBA are already deemed to be in compliance with these requirements. While this requirement applies to businesses of all sizes, data security safeguards may be implemented and maintained that are "appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers." For purposes of the SHIELD Act, a small business is any business with fewer than 50 employees, less than $3 million in gross annual revenue in each of the last three years, or less than $5 million in year-end total assets.

There are potential penalties.

While the SHIELD Act does not provide for a private right of action, the attorney general may bring an action to enjoin violations of the law and obtain civil penalties. For data breach notification violations that are not reckless or knowing, the court may award damages for actual costs or losses incurred by a person entitled to notice. For data breach notification violations that are knowing and reckless, the court may impose penalties of the greater of $5,000 or up to $20 per instance with a cap of $250,000. For violations of the reasonable security measures, the court may impose penalties of not more than $5,000 per violation.

If you have further questions about the SHIELD Act and how it may impact your business, employees, or consumers, please contact a member of our team. – *Jenny L. Holmes*

Cybersecurity

Cyberattacks on construction companies: Why construction companies are vulnerable targets and how they may protect themselves

Special thanks to Courtney Way (Summer Associate) for her contributions to this post.

When we imagine cyberattacks, we often picture hackers breaking into websites and stealing credit card or social security information. We think of companies full of financial or personal information falling victim to these attacks. What we don't often think of is a construction company's information being held hostage, its checks for services being redirected to unknown accounts, or construction equipment being hijacked. Unfortunately, because we aren't expecting these attacks is exactly why construction companies are exposed.

Hackers are learning that the construction industry is a vulnerable target. These companies constantly manage complex projects while handling data exchanges among many parties including partners, subcontractors, regulators, and suppliers. Daily communications between these parties occur over e-mail, providing hackers a perfect opportunity to strike.

Typically, hackers will use a fake e-mail account or even mirror a familiar account in order to ask the company to send funds to a "new" or "different" bank account. Since the communication appears to come from a person that the company deals with on a routine basis, the company assumes that the new bank account is legitimate. Yet, theft of funds is not the only type of cyberattack construction companies may face; hackers also use information to lock data or destroy or control hardware and equipment.

Given the sophistication of today's cybercriminals, construction companies must recognize their risk as targets and begin implementing protective measures. The most important steps for companies to take include: (1) conducting security assessments or routine vulnerability scanning; (2) updating software, including advanced e-mail filtering; (3) enforcing password policies; (4) restricting approval rights and administration privileges; and (5) obtaining cyber liability insurance policies.

However, general liability policies typically do not cover harm suffered by a cyberattack. About a decade ago, companies were unsuccessfully fighting with policyholders about general liability policies covering losses resulting from a data breach. Today, commercial general liability policies generally explicitly exclude electronic data from its definition of "property damage."

Given the need for a policy that would cover the loss of data resulting from a cyberattack, insurance companies began offering separate cyber liability insurance policies. First-party cyber liability insurance typically covers the cost of network business interruptions, forensic investigation and

restoration, legal fees, credit monitoring, and cyber threat extortion expenses. Third-party cyber liability insurance typically covers wrongful disclosure, content liability risks, and security or privacy breach regulatory proceedings.

Companies must be well educated and represented when obtaining cyber liability insurance. Unfortunately, many companies that offer these policies seek to limit their liability and in turn, except many incidences. For example, one policy in 2017 attempted to except costs associated with a fraudulent funds transfer that occurred when employees initiated the transfer after receiving a forged e-mail from a hacker. In 2018, another policy attempted to limit its coverage by arguing that the losses incurred by a company were not directly caused by computer fraud, but rather were incidental. Now, policies are attempting to invoke an "act of war" exception where companies argue that large attacks from foreign hackers are in fact "acts of war" and therefore not covered by the policy.

Although it is recommended that companies obtain cyber liability insurance policies in an effort to combat the enormous expense that follows a cybersecurity breach, cyber liability insurance policies are not a simple catch all and are certainly not an alternative route for staying current on training employees, frequently updating software, and conducting regular security assessments.

While construction companies may not appear to be the most profitable targets for hackers, they are the perfect combination of numerous moving parts, people, and complex projects. Add to this their lax cybersecurity measures, and hackers have found an opportune target.

In order to combat the recent uptick in hackers attacking construction companies, we recommend that companies (1) train employees about cybersecurity; (2) frequently update software; (3) conduct regular security assessments; and (4) look into obtaining cyber liability insurance. A cyberattack could cost millions of dollars and your reputation. In a world where three out of four construction companies have reported a breach in the last year, cybersecurity is not to be taken lightly. *–Jenny L. Holmes*

For more information, please contact:

— Jenny L. Holmes at **jholmes@nixonpeabody.com** or 263-263-1494

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team