CARLTON FIELDS

Risky Business: Common Cyber Security Risks, Expensive Consequences

June 15, 2015

Large-scale data breaches have become increasingly common, bringing with them not only bad press and loss of customer goodwill, but serious monetary risk. New cyber security legislation enacted in multiple states, including Connecticut, Montana, and New Jersey, has also increased regulatory scrutiny and risk. Key causes of data breach risk and liability include:

1. **Inadequate training and employee negligence.** Employees with access to sensitive data who are not adequately trained to identify spoofed websites, phishing emails, or other security risks, may jeopardize their secure credentials, in turn putting sensitive company data at risk. Anthem and Premera Blue Cross, both of which sustained large scale data breaches earlier this year, are believed to have fallen victim to a hybrid spoof-phishing attack called typosquatting, perpetrated by creating and associating an exact copy of an employer's website with a slightly-misspelled version of the employer's URL. A phishing email is then used to redirect employees to the decoy site, where they may unwittingly enter secure credentials. Proper training and employee awareness is essential to avoiding such attacks.

2. **Third-party service providers.** The consumer finance industry outsources certain business functions to third-party service providers. The CFPB, other regulators, and various state laws hold industry members responsible for the actions or inactions of third-party service providers, mandating review and understanding of such vendors' own data security protocols.

   Third parties with access to equipment, infrastructure, and sensitive data, such as maintenance and service companies, are also a source of risk, providing a potential alternative, less secure access point to protected data. For example, the source of the massive Target breach (which resulted in a $19 million settlement with MasterCard), is believed to have been a phishing email sent to Target's HVAC vendor. Inadequate website design can also create risk. After an Illinois bank's website, which had been designed, hosted and maintained by a third-party web developer,

was hacked, the bank had to revamp the website to address the security issues, as well as notify its customers of the breach to comply with state privacy laws. In avoiding such risks, industry must assess and act to protect the security of data in the hands of service providers, guard against potential back door, unintended access through other third-party vendors, and ensure public facing websites are adequately secured.

3. **Malicious insiders.** Needless to say, threats to cyber security may also come from malicious employees. For example, AT&T was recently fined $25 million for failing to prevent the misconduct of a rogue employee which led to a data breach affecting nearly 300,000 customers. Mitigation of this risk requires thorough screening procedures during employee on-boarding, adequate training, supervision, and monitoring. In addition, screening and training policies and protocols must be regularly assessed and updated.

Related Practices

Intellectual Property
Cybersecurity and Privacy