3 Simple Steps to Protect Your Business from Cybersecurity Losses

by: Matt Bergman, Shareholder
Shulman Rogers

PCI Compliance

Review Contracts

Does your business accept credit card payments from customers? Does it purchase products or services from vendors or suppliers? If the answer is "yes" to either of these questions, read on.

Virtually every business that uses a computer with internet access has already been hacked. Fortunately, most businesses have yet to experience the type of cybersecurity breach that could cause it to shut down operations, permanently. And like the next terrorist attack on U.S. soil, it is not a matter of "if" it will happen, but "when" it will happen. So, what can your business do to mitigate the risks and ramifications of an inevitable data breach? Start with these 3 simple steps…

1

If your business accepts credit card payments from customers, make sure your business meets the Payment Card Industry Data Security Standard (PCI DSS). There are 12 requirements for a business to be compliant with the PCI DSS, all of which can best be accomplished by an IT consultant working closely with an experienced information and data security attorney. The requirements include maintaining the most up-to-date software, conducting periodic firewall checks for vulnerabilities and running malware checks on your point-of-sale hardware. It was malware installed on point-of-sale devices purchased and utilized by Target and Home Depot that was responsible for the data breaches they suffered.

2

Have an experienced contracts attorney (a cybersecurity law practitioner is a big plus!) carefully review all of your business contracts, particularly merchant account agreements with banks and credit card processors, service agreements with third party service providers, and supply contracts with vendors and others in the supply chain of your business operations. The contracts must be updated to include cybersecurity-related loss indemnification provisions, data loss and data breach clauses and internet security protocols and requirements. Surprisingly, less than 50% of all business contracts contain such cybersecurity risk mitigation provisions and protections today. Target, Home Depot and Dell all suffered cybersecurity losses

Cybersecurity Insurance

due to inadequate contract protections and protocols with vendors in their respective supply chains. Just a few thousand dollars spent now on a contract review and audit by a qualified attorney could end up saving your business tens of thousands of dollars in cybersecurity losses and damages later. It is also prudent to conduct due diligence on companies that you do business with. Ask your vendors, suppliers and servicers to certify that they regularly undertake proactive measures to protect their data and system integrity.

3

Call your insurance agent and obtain cybersecurity, internet and data loss insurance coverage for your business, all of which are necessary to insure against losses and damages resulting from data breaches and cybersecurity attacks. NOTE: Most insurance policies in effect today (such as those providing general liability, property and casualty, and errors and omissions coverages) DO NOT cover losses resulting from data breaches and cybersecurity attacks. While the premiums for such additional insurance coverage can be costly, those premiums pale in comparison to the potential liability. However, discounts are available for businesses which can demonstrate that they are PCI DSS compliant, that they have updated their business contracts to include cybersecurity risk mitigation provisions and protections, and that they have protocols and practices in place to verify and fully vet companies with whom they do business.

As a former "big firm" partner of a downtown DC law firm, Matt Bergman currently serves as Chairman of Shulman Rogers' Commercial Finance Practice and Co-Chairman of Shulman Rogers' Cybersecurity Practice. Matt utilizes his 20+ years of market knowledge and business deal experience to provide clients with practical advice in two specific areas, cybersecurity and commercial finance - serving as legal counsel for national, regional and local businesses in a variety of industries.

SHULMAN ROGERS | GANDAL PORDY ECKER