masuda funai

News & Types: Client Advisories

"51% of U.S. Based Businesses Targeted by Cyber Attacks - A Checklist to Protect Your Company from Risk"

4/6/2021

By: Kenton P. Knop

Practices: Intellectual Property & Technology

EXECUTIVE SUMMARY

Cybersecurity risks are not a brand-new phenomenon. However, the number of reported cybersecurity incidents has substantially increased as the COVID-19 pandemic caused businesses to rapidly adapt to a work-from-home structure, which created new vulnerabilities as greater numbers of employees remotely connected to business servers. The hard lesson learned from the past year is that businesses of any size can and will be targeted by online criminals seeking to obtain sensitive information, such as business data, social security numbers or credit card information, or to even impersonate company personnel to redirect wire and ACH payments meant for vendors to fraudulent bank accounts.

To help guard against the increased threat of cybersecurity incidents, businesses of any size are strongly urged to consider taking the following steps as soon as possible:

1. **Conduct an IT Vulnerability Assessment.** It is crucial for a business to understand how its online computer network functions and its vulnerabilities, especially the vulnerabilities presented by employees working remotely from home. The business must then promptly address any vulnerabilities identified. Businesses should also consider vulnerabilities created by vendors.
2. **Engage in Employee Cybersecurity Training.** Employee awareness is one of the strongest deterrents against online fraud, as many online fraud incidents attempt to trick or manipulate employees into sending money to a fraudulent account or clicking a link that installs malicious software or provides fraudsters with password access. Because a vigilant employee is often the last line of defense against cybercrime, regular employee training is key to a strong cybersecurity program.

3. **Consider Licensing Next Gen Endpoint Security Software.** Unlike older types of anti-virus software that are updated only after new types of viruses are identified, next gen endpoint security software utilizing AI learning is more likely to quickly detect a cybersecurity issue.
4. **Implement Multi-Factor Authentication.** Implement multi-factor authentication (MFA) on all systems, platforms, and applications that support MFA.
5. **Consider Procuring Cybersecurity Insurance.** Cybersecurity insurance can be critical to offset expenses in the event of a cybersecurity (including ransomware) incident. However, cybersecurity insurance generally must be acquired in addition to standard business insurance and typically is subject to separate underwriting requirements, which means businesses must plan ahead to have such policies in place before an incident occurs.
6. **Back-up Company Data Regularly.** In the event of a cybersecurity incident, crucial data may be locked away (as in a ransomware attack), deleted, or no longer safely accessible due to the bad actor. It is therefore important for businesses to regularly back-up their data in a secure location through a quality provider, preferably off-site or in the cloud, so that data can be quickly restored once the incident has been addressed. Businesses also should consider making the credentials that access those backups different from the primary active directory credentials.
7. **Maintain Physical Security Measures.** Not all cybersecurity incidents occur online. The theft of a company laptop or storage device containing sensitive data from an employee's home, car, or a public place can create its own risks to company data. Strong password protections for access to company devices combined with data encryption measures can help mitigate the risks associated with theft of company property.
8. **Update Company Privacy Policies.** Update company privacy policies to comply with applicable law, including the California Consumer Privacy Act (CCPA), to help minimize the risk of claims/damages in the event of a cybersecurity incident.
9. **Have a Response Plan.** All 50 U.S. states impose some requirement to notify residents of incidents in which their sensitive personal information is disclosed or accessed by unauthorized parties. To comply with state notification requirements in a timely manner, it is critical to identify what information was disclosed or accessed, whose information was affected, and where those individuals reside. Having a cogent response plan in place before an incident occurs can be key.

By taking the above actions, businesses can place themselves in the best possible position to prevent cybersecurity incidents from occurring, or in the worst-case scenario, help minimize the risks and liability that results from a cybersecurity incident and quickly get back to business.

For additional information, please contact Kenton Knop or any other member of Masuda Funai's Intellectual Property & Technology Practice Group.