MERCHANTE

10 Tips to Help You Build Your Business Cyber Security Program

Growing businesses need successful cybersecurity programs to protect themselves and foster trust with their customers. We've compiled a few tips for creating an ironclad security program for your business.

Focus on Security Awareness Training

- Employee mistakes are common contributors to security issues and can be mitigated through training
- Create basic security policies and procedures for employees that detail appropriate Internet use, proper handling of customer information, and physical security
- Provide regular communication regarding cybersecurity best practices and updates

Be Vigilant Against Phishing

- Phishing is a form of cyberattack that tricks the user into sharing private information (passwords, identity, financial info, etc.) by pretending to be a reputable source
- Typical methods used for phishing attacks include email, malicious files/downloads, fake login pages, and fake browser updates
- According to a joint study by IBM and Ponemon Institute, the cost of a phishing attack on a business can be as much as $3.8M

Don't Overlook Basic Network and Device Security

- Implement security controls like firewalls, antivirus, and virtual private networks (VPNs)
- Leverage Managed Security Service Providers to help you outsource important functions that can't be done in-house
- Consider using fintech solutions that include vulnerability scanning as part of your payment card compliance (PCI) solution

Encourage Good Password Hygiene

- Don't reuse passwords across different sites and accounts, and make sure to avoid password defaults
- Use a password vault so you don't have to remember passwords for all your online accounts
- Consider using multi-factor authentication wherever possible

Invest in Insurance

- Protect your business from the impact of a cybersecurity attack by investing in insurance
- There are two types of cybersecurity policies: first-party policies (covering costs associated with a breach of your systems) and third-party policies (cover costs incurred by you when other third parties experience a breach)
- Purchase cybersecurity insurance based on the likelihood of attack and the potential financial impact of the event

Take Your Customers' Privacy Rights Seriously

- Customers today expect their personal data to be safeguarded, so make sure you're up to date with the latest privacy laws and regulations like GDPR and CCPA
- Develop a data protection strategy that helps you stay compliant with privacy laws and regulations
- Appoint a Data Protection Officer to handle incoming requests from customers wanting information about or removal of their data in accordance with "Right to Access," and "Right to be Forgotten" requirements

Keep Customer Payment Information Secure

- Treat PCI compliance as a business-as-usual activity, not a checklist reviewed once a year
- Devalue customer data with tokenization and encryption
- Ensure that your banks and processors are using the latest and most trusted antifraud tools and services

Prepare for the Unexpected

- Develop incident response and business continuity plans
- Test your plans regularly — don't take a "set it and forget it" approach
- Stay on top of the latest industry best practices and trends and update your plans accordingly

Patch Your Systems

- All software requires updates from time to time. Regularly update your systems for the latest bug fixes and security patches
- Take advantage of auto-update functionality where possible
- Implement a patch management program to proactively mitigate vulnerabilities, enhance security, stay compliant, and protect employees and customers

Manage Your Third Parties

- Third-party relationships are necessary for any well-run business, but also introduce risk. Vet your third-party vendors and make sure that you consider cybersecurity during the review process
- Request documentation of services provided and proof of their security and privacy posture. PCI Attestations of Compliance are required from anyone handling payment data on your behalf

As companies continue to move online to conduct business, implementing a sound cybersecurity program is vital to protecting your organization's reputation and financial health.

MerchantE has kept these considerations in mind, and has created a robust financial platform that gives you the protection you need. From PCI compliance solutions to built-in financial breach protection, you can rest assured that we have you covered.

Connect with one of our specialists to learn more about how we can help secure your business while fueling growth.

Let's Connect

MERCHANTE

Call Now! **(866) 663-6132**

Or visit us online at **MerchantE.com**

MerchantE.com | 1150 Sanctuary Parkway, Suite 300,Alpharetta, GA, 30009 |