PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Designing an Effective Cybersecurity Strategy for Private Business Owners

By Thomas J. DeMayo, Partner, Cybersecurity and Privacy Advisory

The cybersecurity landscape is one that is constantly evolving and maturing. Over the past decade, the world has witnessed cybercriminal organizations successfully launch a multitude of attacks with ever-increasing determination and sophistication. In current affairs, the political landscape and the threat of nation state attacks — not just against the government, but also Main Street — has reintroduced a fear long forgotten with the end of the cold war era.

The threat of a cyber-attack is actively lurking over every individual and business, inclusive of those privately owned and operated, big or small. As a privately owned business, many of which may be generational, the stakes are high in protecting your well-established reputation through years of hard work and sacrifice. As a business, you have information of value and, in many cases, your information technology environment may be critical for business operations. As a business, you are going to face the following key cyber threats:

- **Social Engineering** – Your greatest assets, your employees, are being actively targeted by cyber criminals to manipulate them to perform an action. That action, be it clicking a link or supplying information, becomes the foothold the threat actors need to further penetrate and compromise your systems and network.

- **Ransomware** – Cybercriminals, once they gain access, will attempt to take down every critical system you have and make it non-operational. In addition, they will exfiltrate your data and threaten to release it to the public. That data may consist of very sensitive information about your employees, customers and/or your intellectual property. They will stop the attack by requesting large payments in the form of cryptocurrency. Payment demands can be in the millions.

- **Business E-Mail Compromise (BEC)** – Cybercriminals will gain access to mailboxes of your employees, vendors, or customers and leverage that aspect to divert funds. BEC has accounted for $2.7 billion in losses during 2022, according to the FBI. That dollar amount continues to increase year-over-year. In 2014, when this type of fraud was starting to be actively measured, the annual loss was just $267 million.

- **Third Party/Supply Chain Risk** – As a private business, you likely leverage many third parties to facilitate your operations: Cloud storage, cloud applications, outsourced IT network management, phone operations, etc. All these entities present risk to your business operation and data. Just as your business is being targeted, so are all of your third parties. Those third parties become a direct risk to you and a component of your overall risk chain.

According to the U.S. National Security Alliance, 60% of small businesses that are victims of a cyberattack go out of business within six months. For a privately owned business, cybersecurity should be built into the culture of the operations and serve as a natural extension of the duties of the business to operate in the best interest of their stakeholders. Do not make the mistake of considering cybersecurity an expense, instead, embrace it is an investment in the success of your business. In the world of cybersecurity, those who fail to prepare, prepare to fail.

As you evaluate your cybersecurity protections, some best practice considerations to embrace are as follows:

Identify

- Establish the inherent risk of your business. For example, certain businesses may be of higher profile for various reasons or handle larger amounts of sensitive information. The higher the inherent risk, the more robust and advanced cybersecurity program you will need.
- Perform a threat modeling exercise. Such an exercise will also help establish the inherent risk of the business once the threats that exist are inventoried.
- Inventory all IT assets, data locations and service providers. You can't protect what you don't know you have.
- Have an independent cybersecurity specialist conduct an assessment to uncover risks as they relate to the people, processes and technology that make up the overall cyber program.
- Perform penetration testing that is designed to simulate the attacks of a malicious individual.
- If using cloud providers or outsourced IT contractors, ensure you have done adequate due diligence on how well they can safeguard the data and/or access with which they will be entrusted.

Protect

- Perform social engineering tests involving employees to see who is prone to clicking or opening attachments in e-mails, text messages, or engaging in phone conversations.
- Provide security awareness training to all employees.
- Enforce strong and consistent access controls. Passwords should be 14+ characters in length.
- Multi-factor authentication (MFA) should be enabled for any remotely accessible system or application.
- Restrict administrative accounts to a few select trusted individuals.
- Restrict access and ensure least privilege (lowest permission level) to all of the family data.
- Control and prevent lateral movement should an attacker gain a foothold in the business office. In other words, don't let one compromised machine become the pivot point to many other machines.
- Encrypt data at rest and in transit.
- Patch known vulnerabilities.

Detect

- Implement strong malware detection and prevention software.
- Ensure Security Logs are:
  - Captured
  - Stored (minimum of 1 year)
  - Analyzed 24x7 by security operations staff. If you are a small family office, leverage third party services such as a SOC As A Service.
- Alert on what is critical. Many IT operations over-alert and suffer from alert fatigue and critical issues go unaddressed.

Respond

- Have an incident response policy, plan and playbook that will guide the response process and procedures.
- Test the plan by performing a tabletop exercise. This is an exercise where the incident response team is provided a moderated set of scenarios by a security expert to gauge the team's understanding of their roles and the effectiveness of the procedures to be performed.

Recover

- Ensure an effective backup strategy that is designed to be ransomware resilient.
- Maintain a Business Continuity and Disaster Recovery Policy, Plan and Playbook.
- Establish Key Recovery Metrics
  - Recovery Point Objective (How much data can we lose?)
  - Recovery Time Objective (How long can we be down?)
- Test the plan.

An effective cybersecurity program has many moving parts and involves skilled resources that understand the cyber threat, can quantify the risk and design and implement a go-forward strategy. For businesses that may not be able to justify the expense of a full-time Chief Information Security Officer (CISO), a virtual/fractional CISO (a/k/a vCISO) may be a better solution.

Contact Us

At PKF O'Connor Davies, we have a team of cybersecurity professionals and virtual Chief Information Security Officers (**vCISO**s) ready to assist businesses design, implement and manage their cybersecurity program. Let us help protect the very business you have worked hard and long to nurture and support.

Reach out to your PKFOD client engagement partner for referral or contact me directly:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 696.449.6363