CYBERSECURITY

CYBERSECURITY— IS YOUR NETWORK SECURE?

Cyberattacks pose one of the greatest risks to the profitability of businesses in today's economy. Criminals from around the globe are finding cybercrime more lucrative than ever – discovering opportunities to profit off of those who fail to protect the information of their business and customers. You may have heard about some of the high-profile data breaches like Equifax, Facebook and Target, but the reality is that smaller companies are at even greater risk of cyberattacks.

From identifying vulnerabilities in your systems and applications to remediating the weaknesses, Warren Averett can help give you peace of mind. We can help your business take a proactive approach to cybersecurity and minimize the risk of a data breach.

WHY SHOULD YOU INVEST IN CYBERSECURITY?

- Big or small, your data could be at risk. While the data breaches you see on the 6 o'clock news are usually large, multinational corporations, the truth is that over 70 percent of cyberattacks are on small to mid-size businesses. It is easy to believe that a small business would not have a considerable risk due to its size, but every business has valuable information that hackers could use or sell.
- Your system may already be compromised. On average, it takes a business 191 days to identify a breach. Just one breach can cause significant damage.
- Threats can take a variety of forms. From ransomware to malware to phishing, vulnerabilities can be hard to catch without trained professionals looking for them. Even small cracks in the structure of your system can compromise sensitive information.
- Digital theft causes more losses than physical theft. In 2018, the losses recorded from digital assets surpassed those of physical assets. If you have a lock on your door, you should be thinking about putting a lock on your data.
- As your business grows, vulnerabilities increase. The more programs, devices and endpoints that you have on your system increases its complexity. As the system becomes more complex, the higher the risk that a vulnerability will present itself. For any growing business, cybersecurity is a must.

RISK ASSESSMENT

A risk assessment takes a look into your infrastructure to identify weaknesses, as well as risks which can exist independent of vulnerabilities. A risk assessment not only identifies weaknesses and risks, but also how to eliminate your risk. Our experts will provide you with a detailed report as well as suggestions for remediation. This can help your business prioritize what vulnerabilities and risks to focus on and how severe the threats to your business might be.

Warren Averett
RISK, SECURITY & TECHNOLOGY

VULNERABILITY TESTING

A vulnerability test, or vulnerability assessment, is an analysis to review your internal and external network environment. During the test, our professionals look for vulnerabilities, or weaknesses, in your infrastructure through which a cybercriminal could gain access to your system. These assessments will identify what may be at risk and if any further action needs to be taken.

PENETRATION TESTING

While a vulnerability test searches for vulnerabilities in a system, a penetration test attempts to identify weaknesses in an environment. Our Certified Ethical Hackers look for ways to infiltrate your infrastructure as if they were a cybercriminal. If they are able to get in, so can hackers. Tests are run on software and devices within your system to inspect databases, and to search for malicious intrusions, such as adware and spyware. Tests are also performed on various data security measures, including firewalls, anti-virus tools, patches, internal controls, remote access and more.

WEB APPLICATION SECURITY TESTING

What is a web app? A web application is software that runs on a remote server so it does not have to be installed. Some examples of web apps include Google Docs, Mailchimp, Hubspot and Facebook, but there are many more that your organization is most likely using. Web applications are at risk to cyberattacks and could impact the security of your data. Our team can help you identify which web apps should be assessed for security.

AWARENESS TRAINING

Two thirds of all breaches are accidental and could be prevented with solid controls and constant education. Warren Averett offers security awareness training to companies of all sizes. From developing policies to educating your employees, our experienced staff can help ensure your data is safe.

SECURITY COMPLIANCE

Information Security is often required by companies or industries for you to continue doing business with them. Compliance regulations change frequently and are becoming more prevalent—HIPAA/HITECH, FAR, DFAR, PCI, DSS and GCBA to name a few. A comprehensive cybersecurity assessment matches the objective of COBIT, ISO/IEC, NIST, AICPA Trust Services with SOC 2 and SOC 3, as well as regulatory requirements from HIPAA/HITECH to validate the adherence of the compliance your company may need.

SPECIALIZED TEAM CERTIFICATIONS

- Certified Information Security Managers (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Information Technology Professionals (CITP)
- Certified Ethical Hackers (CEH)
- Certified Information System Security Professionals (CISSP)
- Security+
- Certified Public Accountant (CPA)
- Certified Penetration Tester (CPT)
- Web Application Penetration Tester (WAPT)

To learn more about our cybersecurity services and how we can help your business, call us at 800.759.7857 or visit our website at www.warrenaverett.com.

Warren Averett
RISK, SECURITY & TECHNOLOGY