Agility Cybersecurity Services

A.I. verified Penetration Testing as a Service (A.I. verified PTaaS)

Often, companies use one-time consulting engagements to solve their cybersecurity and business continuity problems which gives business leaders a snap-shot of their security posture in that particular moment rather than continual insights into an ever-changing environment. With Agility's A.I. verified PTaaS service, you can choose from a menu of cybersecurity and business continuity services that you would like performed throughout the year. This will help you to:

- Bundle your cybersecurity and business continuity services together in a custom sequence that best suits your business needs
- Gain continual insights into the status of your security posture
- Ensure you are constantly leveraging the latest and greatest technologies and approaches to cybersecurity and business continuity
- Pay a monthly recurring fee with bundled discounts

IT Polices & Procedures Review

Agility can provide written information security policies and procedures and review and test them regularly. The policies and procedures will also meet any industry compliance as well as inventory hardware, software and network resources.

Cyber Network Vulnerability Assessment

Regular Cyber Network Vulnerability Assessments help minimize your security exposure by evaluating existing security policies and plans, general security management processes, evaluation current infrastructure status, and network architecture. After the completion of each assessment, an executive summary will be provided, outlining possible network infrastructure vulnerabilities.

Network A.I. verified Penetration Testing Services

Our A.I. verified Penetration Testing engagements are about reconnaissance and learning as much as we can about your network and how information assets are protected. Our consultants identify threats and potential risks where your organization is a target for compromise. Our engagements are scoped to your requirements and mapped to best-practice A.I. verified Penetration Testing standards.

866-364-9696
contactus@agilityrecovery.com
www.agilityrecovery.com

Cyber Incident Response Planning

Cybersecurity breaches are commonplace today for businesses of all sizes. The impact can be significant, creating financial, reputational, and personal data exposure risks to an organization and customers. Regulatory bodies have tightened up requirements for data breach response, notification procedures, security policies, and the protection of personal data. Agility has the professional experience to develop an incident response plan that addresses critical actions including preparation, identification, containment, eradication, recovery, and remediation procedures. Incident response team training and scenario based tabletop exercises provide the necessary instruction on how to prepare for and respond to a data breach through collaboration of team resources.

Third-Party Vendor Assessment / Due Diligence Questionnaire (DDQ)

Organizations are increasingly contracting with vendors to gain a competitive edge, enhance product offerings and reduce costs. Today's businesses must have a clear understanding of the risks inherent in their business relationships with outside parties. To address these risks, companies must implement programs using third-party risk management strategies to understand and mitigate its risks effectively. Establishing an effective vendor risk program for contracting with and monitoring service providers can be a means of fortifying risk management initiatives, especially for organizations that face significant regulatory oversight, cybersecurity, and privacy concerns. Agility provides a comprehensive set of tools, processes and professional expertise to assess vendor relationships that align with regulatory expectations and deliver intuitive assessment results.

Written Information Security Program ("WISP")

A Written Information Security Program ("WISP") creates effective administrative, technical and physical safeguards for the protection of personal information of organizations to comply with ISO standards, as well as include guidance and concepts from other industry standards included in the NIST Cybersecurity Framework.

The WISP will define an organization's procedures regarding electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting confidential information. The WISP is developed to include the following key features, requirements and components:

- Identify internal and external risks to the security, confidentiality, and/or integrity of records containing confidential information
- Assessment of potential damage of these threats, taking into consideration the sensitivity of the confidential information
- Evaluation of the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks
- Design and implementation of safeguards to minimize identified risks

With an end-to-end solution, such as Agility Recovery, businesses can recover **4 times faster** than with no BCM solution.

Agility Recovery

866-364-9696
contactus@agilityrecovery.com
www.agilityrecovery.com

Agility Recovery provides everything needed to **prepare, test,** and **recover** from any interruption.