BARCODE

WE CYBER.

2025 SERVICE CATALOG

PROTECTING SMES WITH CUSTOMIZED SECURITY EXPERTISE

ABOUT US

BARCODE is a leading cybersecurity firm that has grown from security engineering roots into a multifaceted company offering a comprehensive suite of services. As a cybersecurity ecosystem built by veteran engineers with an innovative perspective, we are dedicated to protecting small and medium-sized enterprises (SMEs) through niche expertise and proven solutions. By offering tailored Strategic Advisory, Penetration Testing, and Awareness Training services, we help organizations stay secure, compliant, and resilient against aggressive threats. Our bespoke services help SMEs reduce risk, validate their defense controls, meet regulatory requirements, and form a security-minded culture. We help support many industries, including:

- **Healthcare**
- **Financial Services**
- **Real Estate**
- **Hospitality**
- **SLED**
- **Retail**
- **Entertainment**
- **Manufacturing**
- **Utilites**
- **IT Services**
- **Pharmaceutical**
- **Private Equity**
- **Legal Services**
- **Transportation**
- **Construction**
- **MANY MORE!**

CONTACT US

www.barcodesecurity,.com

(302) 918 5441

info@barcodesecurity.com

company/barcodesecurity

STRATEGIC ADVISORY

With an end-user focused strategic advisory and landscape navigation, we reduce risk and friction in small-medium enterprises, BarCode provides you the following:

- **Reduced Exposure To Threats**
- **Resource Optimization**
- **Improved Partner Relationships**
- **Operational Resilience**
- **Greater Competetive Edge**

vCISO

Our vCISO services offer executive-level security leadership and continuous guidance to support SMEs without the expense of a full-time CISO. We provide real-time responses using sophisticated risk measurement and compliance automation tools. With continuous assessments and targeted guidance, our experts help develop your security program for a successful journey through today's modern security landscape.

RISK ASSESSMENTS

We conduct comphrehensive Security Risk Assessments, identifying vulnerabilities and aligning risks with compliance standards like HIPAA, PCI, and GDPR. Our evaluations strengthen security controls, prevent costly incidents, and optimize resource allocation, reducing overall risk exposure.

FRAMEWORK ALIGNMENT

Aligning with standards like NIST CSF and CIS involves comprehensive evaluations to clarify Framework compliance. This approach identifies gaps and provides tailored recommendations to strengthen controls, reduce risk, and enhance cybersecurity posture in line with industry best practices.

3RD PARTY RISK MANAGEMENT

Evaluate and mitigate risks introduced by external vendors or business partners, validating alignment with stringent security standards. By hardening controls within your supply chain, we reduce overall risk exposure and protect your business from potential breaches caused by undetected third-party vulnerabilities.

DARK WEB MONITORING

Continuously scan hidden online channels for leaked credentials, sensitive data, and potential threats targeting your organization. By identifying risks early, we help you proactively mitigate breaches and protect your business from cybercriminal activity.

AI STRATEGY

Built on NIST's AI Risk Management Framework (AI-RMF), our AI Risk Strategy mitigates vulnerabilities in AI deployments. We ensure compliance and data protection while securing the integrity of your AI systems, reducing the risk of breaches, ensuring privacy, and surfacing AI-related threats within your enviornment.

BUSINESS RESILIENCY

Our Business Resiliency program encompasses continuity planning, disaster recovery, and incident response. We ensure that your organization can withstand disruptions and recover quickly from unforeseen events, keeping operations running smoothly.

ADVERSARIAL EMULATION

Our comprehensive testing services mimic cyberattackers to provide actionable insights to reinforce your organization's security posture and reduce operational risks, thus achieving:

- ✓ **Vulnerability Mitigation**
- ✓ **Improved Organizational Aware**
- ✓ **Enhance Incident Preparedness**
- ✓ **Validate Process and Procedure**
- ✓ **Develop Defensive Resource Allocation**

PENTESTING

Penetration testing simulates real-world attacks to identify vulnerabilities in your organization's systems before real threat actors can exploit them. This process strengthens security, reduces risk, and validates your existing defenses. We offer internal, external, web app, wireless, IoT, cloud, and API testing.

PHYSICAL INFILTRATION

Physical and social engineering testing assess your organization's physical security and employee awareness, identifying gaps and vulnerabilities. These tests simulate unauthorized access attempts and manipulation tactics, evaluating the effectiveness of safeguards like locks, guards, surveillance systems, and access controls.

TABLETOP EXERCISES

Simulate cyber incidents to test your organization's readiness and response strategies. These exercises help identify weaknesses in your incident response plan, improve communication during a crisis, and ensure your team is prepared to handle realistic catastrophies efficiently and effectively.

AWARENESS TRAINING

SMEs often lack comprehensive security measures, making them attractive targets for cybercriminals looking for easier vulnerabilities to exploit. Security Education will help with:

- ✓ **Minimize Risk of a Successful Cyberattack or Breach**
- ✓ **Reduce Financial or Reputational Damage**
- ✓ **Increase Protection of Sensitive Data**
- ✓ **Strengthen the Human Element**
- ✓ **Add Business Value For Cyber Insurance Providers**

LIVE VIRTUAL SESSIONS

Our live virtual cybersecurity training is engaging, interactive, and designed for retention, with original slides and concise sessions under one hour. We focus on participant involvement and use platforms like Zoom for effective delivery, helping organizations build a sustainable, security-aware culture

ON-DEMAND LIBRARY

Our On-Demand Training offers flexible, self paced learning to meet your needs. We divide 1 hour classes into 15 minute micro-lessons, aligning with typical attention spans for effective, easy absorption. Learners can access training anytime, fitting it into their schedules to gain essential cybersecurity skills without the burden of lengthy sessions.

FULLY MANAGED PROGRAM

A holistic, continous program that provides content, assessments, and ongoing program management to establish and maintain a security-minded culture from the ground up. This “A to Z” approach aims to keep your workforce proactive in recognizing and responding to evolving and trending threats.