CYBERGAPS® SECURITY ASSESSMENT

ENSURING REASONABLE AND EFFECTIVE SECURITY FOR SMALL AND MEDIUM ENTERPRISES

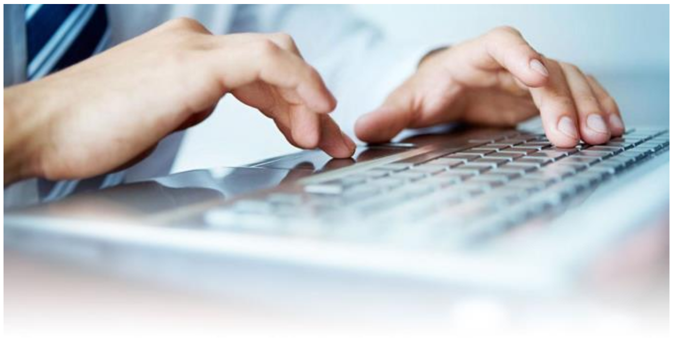
Small and medium enterprises now recognize that a cyber attack may constitute existential risk. Schools, municipalities, hospitals, hotels, law firms, ecommerce merchants, non-profits: cyber criminals do not care about the size of their target if there is a vulnerability that can be exploited for financial gain. As larger enterprises shore up their security infrastructures, criminals are turning to smaller organizations.

Cyber risk is multi-faceted. There is the immediate risk of financial loss if a ransomware attack renders the organization inoperable. There is the direct financial risk of account takeover, wire transfer fraud, or credit card skimming. But there is also third-party risk: the possibility that your customers will sue for failure to protect personal information or that regulators will levy fines for failure to take reasonable precautions.

THE CHALLENGE

How susceptible is your organization to a cyber attack? How capable are your defenses of repelling an attack? How resilient is your organization if an attack gets through? Are the decisions you have made regarding your cyber defenses reasonable? Would they be defensible in the event of litigation or regulatory scrutiny? Vulnerability scanners and penetration tests offer partial answers to these questions. But these approaches have technical blind spots. They are not suited for assessing the human dimension. And remember: the bad guys only need to find one chink in the armor.

To get comprehensive answers to these questions, organizations need to conduct a risk and controls assessment. But smaller organizations are at a loss where to start. The task seems overwhelming. Risk assessment methodologies and security control frameworks, whether they are based on the International Standards Organization, the National Institute for Science and Technology, or the American Institute of Certified Public Accountants, are complex and time-consuming. And when does the organization know that it has done enough?



THE SOLUTION

This is where CyberGaps® comes in. CyberGaps® is a comprehensive but light-weight risk and controls assessment designed for small and medium enterprises. A CyberGaps® assessment provides a full gap analysis and prescriptive guidance for filling the gaps and ensuring reasonable and effective security. It uses multiple choice questionnaires to assess your organization’s risk of information compromise and identify gaps in your organization’s defenses. It then uses a math-based Knowledge Management System to describe and prioritize the security controls to mitigate those gaps.

CyberGaps® prioritizes controls based on security effectiveness. In the medical and pharmaceutical field, the most effective treatments and medicines are based on statistically-based or outcome-based studies. The same is true in the field of cybersecurity. The most effective security defenses are those that have demonstrated the power to block or mitigate real attacks. CyberGaps® calculates the relative efficacies of different controls from threat intelligence and data breach statistics. No other solution on the market offers this capability.

CyberGaps® also identifies controls that may be expected by litigators and regulators in order that the organized be deemed "reasonable". It does this by tracking both cross-sector and industry-specific customary norms. Firewalls and anti-virus systems are expected of all organizations. But in some industries, regular vulnerability scans and penetration tests are also expected. And in others multi-factor authentication and encryption have started to become de facto best practices.

What percentage of gross annual revenues are organizations in your sector spending on security? What percentage of organizations are implementing an anti-phishing solution or secure email gateway? CyberGaps® provides answers to these questions and ensures that your own defenses do not deviate significantly from standard industry practice.

Finally, for those organizations that are subject to specific regulations such as PCI-DSS, HIPAA, or GDPR, a CyberGaps® assessment can be modified to include the relevant compliance questionnaires. These involve simple yes/no responses that answer the question "are we compliant?" but do not provide insight into security effectiveness. Compliance regimes are typically several years behind the curve. Being compliant doesn't make you secure. A CyberGaps® assessment ensures that you do not fall into this "compliance trap". It empowers you to achieve not only compliance but also reasonable and effective security against current threats.

BENEFITS

Following consultation with our assessors that can span up to one day, we analyze the results and present our findings and recommendations to your executives. Our presentation is accompanied by a comprehensive report that provides the following benefits:

- Identifies your areas of highest cyber risk
- Enumerates gaps in your cyber defenses
- Prioritizes your remediation efforts
- Ensures return on your security investment
- Demonstrates cyber due diligence

THE BOTTOM LINE

Ultimately, organizations have to make decisions on how they invest their security budget. CyberGaps® provides a defensible framework for making those decisions and getting the biggest bang-for-the-buck.

eosedge Legal is designed for the Cyber Age, offering interdisciplinary cyber risk and cyberlaw solutions. With our cyber intelligence vendors, malware researchers, and advanced cyber operations teams, **eos**edge Legal brings cyberlaw and services innovation to fill a gap in the market. Our ancillary services model affords clients a complete set of pre-breach and post-breach cyber services.

eosedge Legal
90 South Cascade Ave,
Suite 1100,
Colorado Springs,
CO 80903
PHONE: 719.357.8025
EMAIL: info@eosedgelegal.com
WEB: www.eosedgelegal.com

Legal and ancillary service locations:

Boston,
Denver,
Menlo Park,
San Francisco,
Washington, DC.

CyberGaps® is based on a proprietary Knowledge Management System (patent-pending). See separate product datasheet for details.