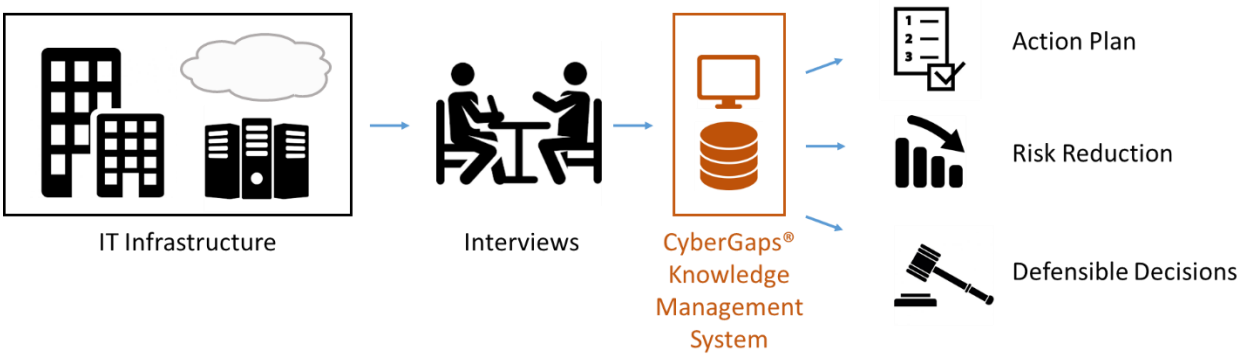
THE CYBERGAPS® KNOWLEDGE MANAGEMENT SYSTEM

ENSURING REASONABLE AND EFFECTIVE SECURITY FOR SMALL AND MEDIUM ENTERPRISES

THE CHALLENGE

Advising a small and medium enterprise on cybersecurity is a challenge. The enterprise may not have the bandwidth to undergo a traditional risk analysis. Evaluating assets, anticipating events that might threaten those assets, and quantifying the likelihood and possible impact of these events is a difficult task. And the enterprise may not have the resources to submit to a traditional controls assessment. Control frameworks and compliance regimes were designed for large enterprises. They are large and complex, often involving hundreds or even thousands of security controls. There is little guidance for those with limited budgets on ranking one control over another. Control descriptions are generic and amorphous, lacking prescriptive detail. It seems like a lot of effort for only minimal gain.



THE SOLUTION

The CyberGaps® Knowledge Management System (KMS) was specifically designed to address these problems. Using patent-pending technology it facilitates the concise assessment of risk and controls at a small or medium enterprise. Instead of requiring estimates of the likelihood and impact of threat events, the CyberGaps® KMS uses proxy measures that are easy to understand, based on the enterprises' attack surface and digital assets. Instead of using a huge one-size-fits-all framework, the CyberGaps® KMS assesses only those controls that are pertinent to the enterprise's risk. Instead of the typical binary scoring (a 1 for "yes", a 0 for "no"), the CyberGaps® KMS provides ratings for incremental levels[1] of control maturity according to estimates of security effectiveness. And instead of vague descriptions, controls come with detailed implementation guidance and recommended vendor solutions.

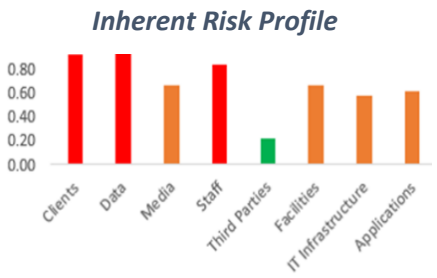
THE INTERVIEWS

The CyberGaps® KMS was designed for cybersecurity assessors. It facilitates the collection of responses to interviews, the quantification of risk and control maturity, the aggregation of risk and control maturity into meaningful groups, the visual identification of security gaps, and the automatic creation of a list of concrete steps for remediating those gaps and demonstrating due diligence. There are eight interviews. Each interview takes between thirty and seventy-five minutes and can be conducted onsite or remotely. Responses are either multiple choice, free form, or a hybrid, depending on the assessor's preference.

[1] There are three levels of maturity for each security control. Each level typically corresponds to a sub-control within the NIST SP 800-53 control catalog or the CIS Critical Security Controls.

ASSESSING INHERENT RISK

The first interview explores the enterprise's inherent risk of information security compromise. The focus is on the type and volume of the enterprise's digital assets and on the business operations and IT infrastructure used to collect and process these assets. It is sector-specific and is used to ascertain where on the spectrum of risk for the sector the enterprise lies. Upon completion, the CyberGaps® KMS issues a risk rating for the enterprise and displays a graphical representation of risk in the "inherent risk profile".



ASSESSING CONTROL MATURITY

The remaining seven interviews document the organization's information security controls, both management and technical. See the table for details.

GOVERNANCE AND OVERSIGHT

The foundation of good cyber hygiene is leading by example. Define board-level responsibility. Define and enforce security policies. Conduct risk assessments to focus investment in the areas of highest risk. Purchase cyber insurance.

INFRASTRUCTURE HARDENING

A lot of wasted effort can be spared by first reducing the attack surface. Eliminate unneeded software and protocols, whitelist "known good" software and scripts, standardize secure configurations, and patch continuously.

BLOCKING AND FILTERING

Keep out the bad. Let in the good. This is the tactical blocking and tackling carried out by firewalls, antivirus, spam blockers, web filters, intrusion prevention systems and anti-phishing protection.

ACCESS CONTROLS

Half of all data breaches involve stolen credentials. Teach users to use long pass phrases or better still use a password manager. Require a second factor for remote access. Minimize the use of administrator privileges. Verify and dual authorize wire transfers, payments and W2 requests.

DATA PROTECTION AND PRIVACY

Maintain off-network backups which are not accessible by ransomware. Segment data according to sensitivity. Allow personal email and cloud services on the guest network only. Enable easy encryption of sensitive emails and attachments. Enforce encryption of removable devices, laptops and mobile phones. Gather consent when collecting personal information. Respond to data subject access requests. Retain sensitive data only as long as there is a business need.

EXTERNAL DEPENDENCIES

As more firms move data to the cloud it is vital to clarify with your providers who is responsible for what. Turn down providers who do not satisfy your due diligence checklist. Lock down access to storage buckets. Require multi-factor authentication. Ensure contracts are watertight and perform regular audits.

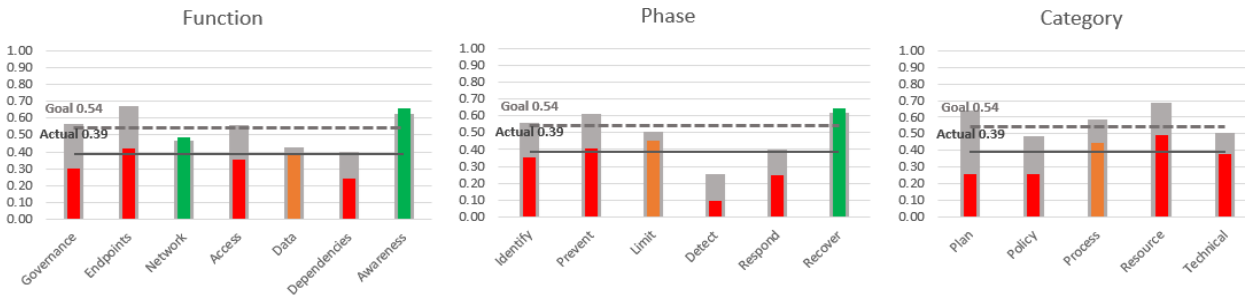
SITUATIONAL AWARENESS

Know your enemy. Know yourself. Keep up with the changing threat environment by joining an information sharing community. Regularly train and test your staff to recognize social engineering attacks. Conduct frequent vulnerability assessments and table-top exercises for your incident response plan.

Management functions include governance (resources, plans, policies, processes), dependencies (management of third parties), and security awareness (cognizance and training). Technical functions include endpoints (system protection), networks (local area, internet, and cloud), access (authentication and permission), and data (protection, recovery, and privacy). The number of controls evaluated in each interview scales according to the enterprise's risk rating and can vary from a handful to around thirty. When a prescribed control or maturity level does not match the enterprise's environment the assessor can replace it with a compensating control.

Depending on customer preference the assessor can conduct a summary or detailed assessment of each control. For a summary assessment the enterprise simply chooses the appropriate level at which the control is implemented, how broadly it is implemented, and whether it is documented and subject to oversight. Customizable defaults are provided to simplify responses. The goals of a summary assessment are to assess the enterprise's defenses, identify gaps and propose remediations. A detailed assessment goes further and includes an educational component. For a detailed assessment the enterprise can use the CyberGaps® KMS and the assessor's knowledge to drill down and explore possible alternatives or improvements to the current implementation.

The CyberGaps® KMS includes extensive documentation for each control. For security policies sample content is provided. For security procedures best practices are recommended regarding frequency and approach. For resources industry best practices for budgeting, staffing and insurance are available. For security technologies practical hints are provided to help with implementation and leading market solutions are listed. Where applicable the CyberGaps® KMS provides guidance from the U.S. National Security Agency or the Australian Signals Directorate and documentation for the corresponding sub-controls within the NIST SP 800-53 catalog and the CIS Critical Security Controls.



AGGREGATING RESULTS

Upon completion of the security control interviews, the assessor needs to ensure that each applicable control is given a maturity rating. When a predetermined multiple-choice response has been selected, the CyberGaps® KMS automatically calculates the maturity rating for the control. When, instead, a compensating control has been documented, the assessor must provide a rating, using her own judgment and the ratings for predetermined responses as a benchmark.

Once all relevant controls are assessed and rated, the assessor can now turn to analysis and reporting. The CyberGaps® KMS aggregates control ratings into meaningful groups to create a comprehensive view of the enterprise's control maturity along three dimensions: a functional view, a lifecycle view, and a category view. A well-balanced risk reduction program will ensure that no significant gaps exist in any of these dimensions.

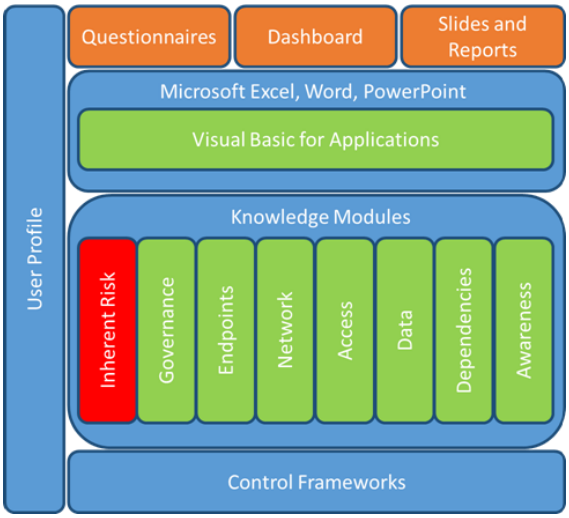
For each group the CyberGaps® KMS enumerates the expected and actual maturity ratings and displays these values in a simple color-coded bar chart on the dashboard. For example, in the maturity profile above, the organization is exceeding expectations for recovery controls, is falling just short for limiting controls, and has significant gaps in the identify, prevent, detect and respond phases of the extended NIST lifecycle. From the dashboard the assessor can examine the maturity of any group, identify which controls need improving, and drill down into the specific details of each control. Analyzing gaps in this manner ensures that the assessor keeps the big picture in mind and does not lose the forest for the trees.

PRESENTING AND REPORTING RESULTS

To facilitate communication with the enterprise's senior management, the CyberGaps® KMS automates the generation of report and slide content using templates. Auto-generated content includes graphical and tabular summaries of the organization's risk and maturity ratings and lists of the recommended management and technical control improvements. Recommendations are accompanied by implementation and market guidance. Templates include sample language and graphics which can be used for an executive summary and project plan. The report and presentation capabilities within the CyberGaps® KMS expedite much of the labor-intensive work of an assessment.

CUSTOMIZATION

To enabled tailored assessments, the CyberGaps® KMS includes a user profile in which the assessor can set various defaults, including ratings, color thresholds, remediation algorithms, and report parameters.



TECHNOLOGY

The CyberGaps® KMS is installed as an on-premise Microsoft Office application running on Microsoft Windows. The user interface and data storage is based upon Microsoft Excel. Knowledge modules for risk factors and security controls are codified in hidden worksheets. Documentation for the NIST and CIS control frameworks is also stored in hidden worksheets. Program logic is based on Microsoft Excel as well as functions and procedures written in Visual Basic for Applications (VBA). Reports are created in Microsoft Word and Adobe PDF format and slides in PowerPoint format using VBA procedures.

---

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.

Copyright 2020 **eos**edge Legal. All rights reserved. CyberGaps® is a registered trademark of Non-State Threat Intelligence, LLC. CyberGaps® is the name of a security assessment service that uses the CyberGaps® KMS and is offered by **eos**edge Legal. See separate solution brief for details.