ebryx

Essential Cyber Hygiene for Small and Medium-Sized Enterprises

Email
securenow@ebryx.com

Essential Cyber Hygiene for Small and Medium-Sized Enterprises

Overview

Small and medium-sized enterprises (SMEs) are increasingly vulnerable in today's fast-evolving digital landscape. In fact, according to recent research from Accenture, 43% of cyber-attacks are aimed at SMEs, but only 14% of these businesses are equipped to fend off such threats. This gap underscores an urgent need for tailored cybersecurity strategies that address the specific challenges faced by SMEs.

Both SMEs and larger corporations operate within the same digital environments, using the same services and infrastructure, and therefore are susceptible to the same cyber threats, sharing equivalent risks and attack surfaces. However, SMEs lack the necessary security resources compared to larger organizations, placing them at a heightened risk of cyber-attacks.

There is no shortage of cybersecurity guidelines, frameworks and standards. Market analysts offer their opinions on security architectures and technologies and thousands of product vendors pitch their products as solutions to cybersecurity challenges. This makes it very hard for SMEs to figure out where to begin and what to prioritize.

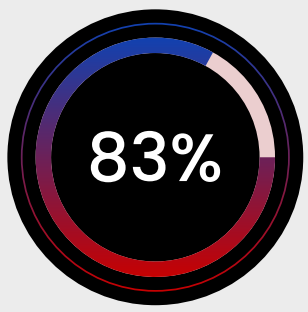
The Center for Internet Security (CIS) Community Defense Model is meant to address exactly the question of what to do first. Among the various security frameworks and standards that are often abstract and complex (NIST 800-53 has 1000+ controls, for instance), CIS Controls are the most oriented towards SMEs and are directly translatable to concrete operational measures. CIS has specified 18 Controls consisting of 153 Safeguards. The CIS Community Defense Model groups these Safeguards into three Implementation Groups with each Group representing progressively more advanced Safeguards that build upon the previous Group. Implementation Group 1 (IG1) is what CIS calls essential cyber hygiene. According to CIS, IG1 is "applicable to even the smallest and least funded enterprises" and consists of "the Safeguards that we assert that every enterprise should deploy".

Unlike most guidance on cybersecurity, the CIS Community Defense Model is evidence-based. Analysis of a large compendium of real-world breach data from sources such as Verizon and Microsoft, combined with the MITRE ATT&CK knowledge base to find the highest impact mitigations against top threats, yields the Implementation Groups, with the most basic and foundational Safeguards in IG1. IG1 consists of 56 Safeguards. These are about one-third of the total CIS Safeguards but protect against more than 80% of the attack techniques used by top threats such as ransomware. Hence, implementing essential hygiene yields the greatest mileage from a limited security budget. For enterprises seeking compliance with SOC 2, ISO 27001, HIPAA etc. investment in IG1 is the logical first step, since all the Safeguards map to requirements from these frameworks. However, the task of implementing all 56 CIS IG1 Safeguards can be daunting, as these can possibly be mapped to 16 or more different types of tools and the development of a dozen or more processes and policies.

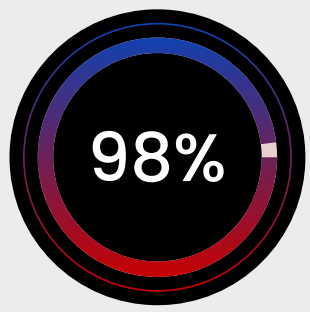
That's where Ebryx comes in. Our Essential Cyber Hygiene Solution covers all 56 Safeguards using a minimal set of versatile tools. Additionally, it includes the creation of the necessary processes, policies, and security leadership and management in a single comprehensive service. Unless a business is just starting out, an enterprise would already have coverage of several essentials in place. However, in our experience, most SMEs have less than 10% coverage of these essentials. Regardless of the current level of implementation, our solution is typically able to fill the gap with just one or two additional tools and a single bundle of our services, providing a solid foundation on which to build more advanced security, should the organization have the need.

This e-book delves into the specific cybersecurity challenges SMEs face, the broader implications of these vulnerabilities, and the steps they can take to build a robust security foundation using the CIS IG1 Essential Cyber Hygiene Safeguards. By the end of this guide, you'll have a clearer path to protecting your business and fortifying your defenses against cyber threats.

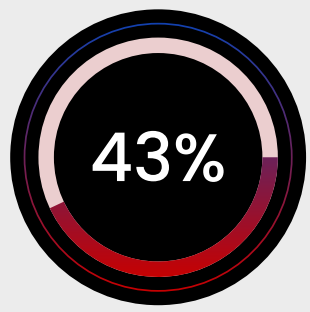
SME Cybersecurity Landscape



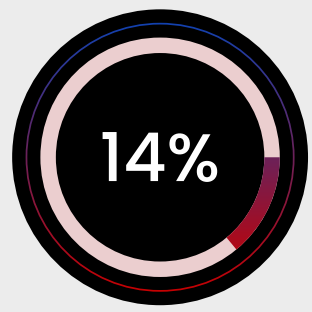
83% of small US business are not financially prepared to recover from a cybersecurity attack. (Mastercard)



Basic cybersecurity hygiene can protect against 98% of attacks. (Microsoft)



43% of cyber-attacks specifically target SMEs. Accenture



Only 14% of affected SMEs are prepared to defend themselves. Accenture

Chapter 1

Cyber Security Challenges Faced by SMEs

Small and medium-sized enterprises (SMEs) are increasingly becoming targets for cyber-attacks, this underscores the critical need for robust cyber hygiene practices among SMEs to protect their valuable data and maintain business continuity. Understanding the unique cybersecurity challenges faced by SMEs is the first step towards implementing effective defenses. To effectively combat these threats, SMEs must recognize and address the following cybersecurity challenges:

Navigating the Complex Cybersecurity Landscape

The cybersecurity market is vast and intricate, making it difficult for SMEs to navigate. With countless solutions and services available, determining which ones are genuinely beneficial can be overwhelming. Many SMEs lack the resources to conduct thorough evaluations, leading to decisions based on incomplete information or marketing hype rather than actual efficacy. This complexity can result in the adoption of suboptimal security measures that do not adequately protect against the specific threats faced by SMEs.

Lack of Evidence-Based Security

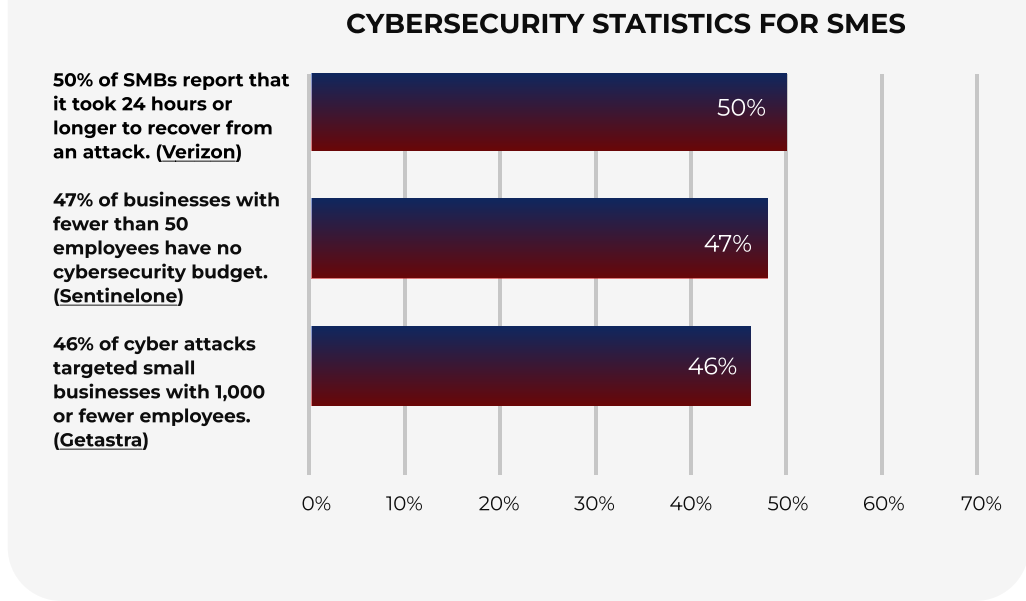
There are thousands of security product vendors and, for instance as in NIST 800-53, over a thousand security measures that an organization can adopt. Which security measures should an SME focus on with its limited budget? Instead of blindly following trends and vendor and market analyst hype, security measures need to be based on reliable data on what are the prevailing attacks of greatest concern and what countermeasures are proven to protect against them.

Compliance Requirements

SMEs providing services or products to large enterprises are increasingly required by their enterprise clients to provide evidence of cybersecurity maturity. SOC 2 and ISO 27001 certifications are a common expectation. Segments such as fintech and healthtech have more stringent compliance requirements with compliance regimes such as PCI DSS and HIPAA. The cost and time of achieving these compliances is a significant burden on SMEs.

Investment vs. Results

Despite increasing their investments in cybersecurity, many SMEs continue to face significant security challenges. This suggests a disconnect between the amount of money spent on security and the effectiveness of the implemented measures. The lack of visible results can lead to frustration and skepticism about the value of cybersecurity investments, potentially resulting in underfunding of essential security initiatives.



Abstract Security Standards

Many security standards and regimes are too abstract and not easily applicable to the specific context of SMEs. These standards often lack clear, actionable steps, making implementation difficult for organizations with limited cybersecurity expertise. For instance, NIST 800-53 has more than 1000 controls. As a result, SMEs may struggle to comply with these standards, leaving them vulnerable to cyber-attacks despite their efforts to adhere to best practices. The complexity of these standards can lead to confusion and incomplete and ineffective implementation. There is a need to make achieving compliance easy and maximize its real impact on security.

Overlooked Needs of SMEs

The cybersecurity market often overlooks the specific needs of SMEs. Many vendors design their solutions for larger enterprises, resulting in products that are too complex or expensive for smaller businesses. This misalignment leaves a gap in the market for affordable, effective cybersecurity solutions tailored to the unique challenges faced by SMEs. Consequently, SMEs may resort to using inadequate tools or forgoing critical security measures altogether.

Expertise and Focus Gap

A significant barrier to effective cybersecurity for SMEs is the lack of specialized expertise and security focused leadership at the top. Many SMEs do not have CISOs and the role is filled by IT and engineering functions on an ad hoc basis. According to a survey by the Ponemon Institute, 70% of Chief Information Security Officers and other IT security professionals worry most about the lack of competent in-house staff when defending their companies against cyber-attacks. Further, 65% of these respondents cite inadequate in-house expertise as the top reason they are likely to experience a data breach. This expertise gap makes it challenging for SMEs to implement and maintain robust cybersecurity measures. This is compounded by the lack of focused, independent, top-level leadership roles focused on security. For SMEs in segments such as fintech, health tech and SaaS filling this leadership and skills gap is critical. Without access to knowledgeable professionals, SMEs are at a higher risk of falling victim to cyber-attacks.

The Solution: Center of Internet Security's Essential Cyber Hygiene Safeguards

Addressing cybersecurity challenges for SMEs requires practical and tailored strategies. Simplifying security solutions and choosing tools that fit their operational needs is essential, avoiding the complexities of enterprise-level solutions.

Optimizing investments through data-driven measures ensures that cybersecurity spending results in tangible improvements by prioritizing threats and vulnerabilities. Implementing practical, clear best practices and operational measures relevant to SME operations, rather than abstract frameworks, makes compliance have more real impact on improving security.

The Center of Internet Security's (CIS) Essential Cyber Hygiene IG1 Safeguards provide a simple means to tackle the challenges discussed. These 56 safeguards, distributed across 15 controls, offer a practical, evidence-based framework specifically designed to provide a solid security foundation. Before delving into the details of each control, it's crucial to understand the significance of implementing the CIS IG1 safeguards.

Understanding Center of Internet Security's (CIS) Implementation Group (IG1) Safeguards

CIS Implementation Group 1 (IG1) serves as "Essential Cyber Hygiene," providing a vital baseline of cybersecurity measures. CIS IG1 safeguards effectively address challenges faced by SMEs by providing a set of practical and manageable measures and protect against more than 80% of the attack techniques used by top threats.

> *Implementation Group 1 (IG1) is the group [of Safeguards] that is least costly and difficult to implement, is what we call essential cyber hygiene (formerly basic cyber hygiene) and are the Safeguards we assert that every enterprise should deploy – CIS CDM v2.0*

IG1 safeguards are crafted to maintain business operations without significant downtime, a common concern for smaller enterprises.

By adhering to IG1, which is considered the least difficult and least costly to implement, businesses can establish a robust defense against the most prevalent cyber threats, laying the groundwork for more advanced cybersecurity practices as they grow.

Why CIS “Essential Cyber Hygiene” IG1 Safeguards Matter?

Relevance and Simplicity

CIS Controls are designed with the specific needs of SMEs in mind, ensuring that they are both relevant and straightforward to implement. Unlike more complex frameworks that may overwhelm smaller organizations, CIS IG1 provides clear, concise and prioritized guidelines.

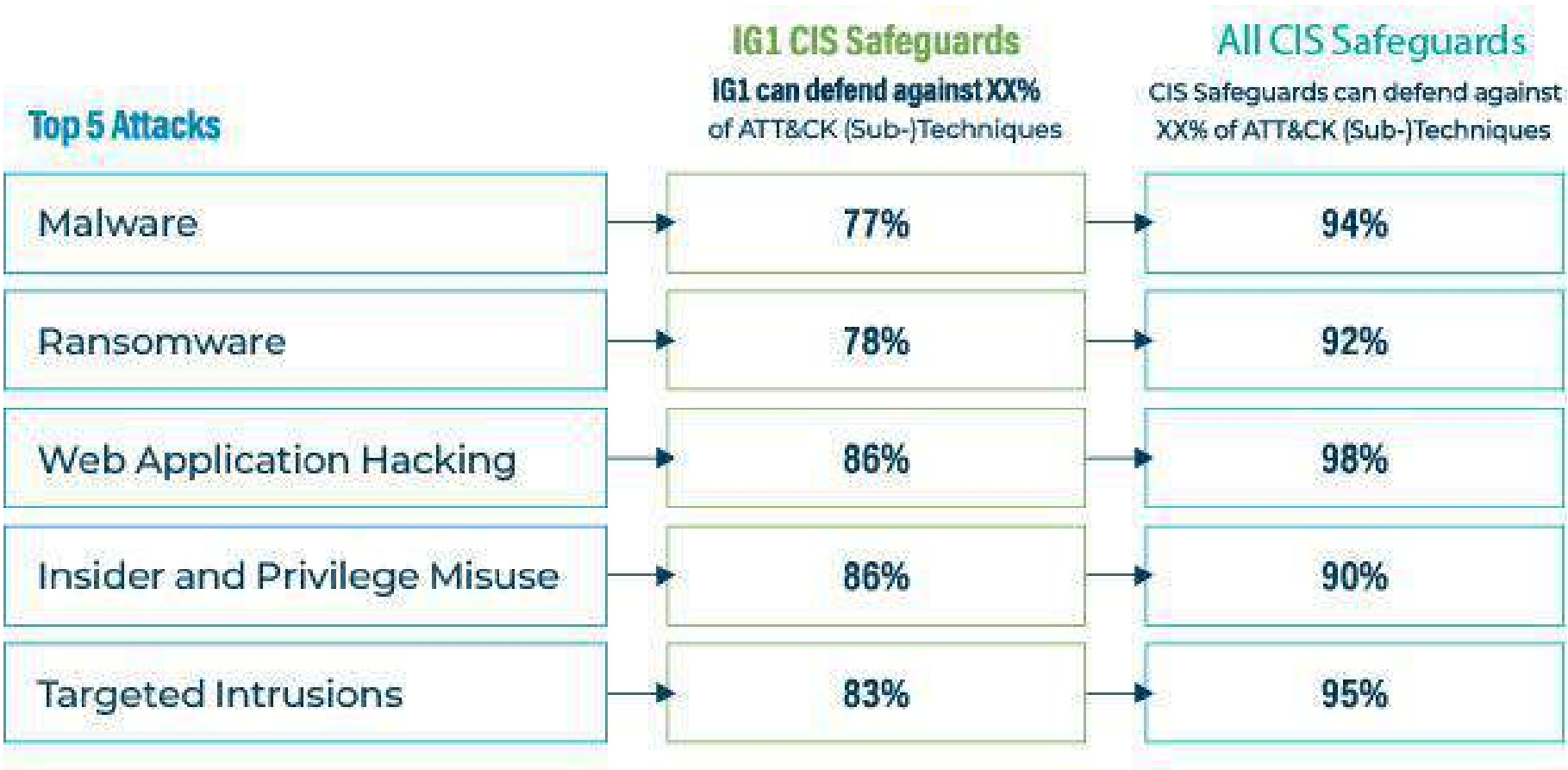
Operational Focus

The CIS IG1 controls are highly operational, focusing on practical, actionable steps that SMEs can take to enhance their security. This includes basic yet crucial measures such as inventorying hardware and software, implementing secure configurations, and managing user access. By emphasizing operational tasks, CIS IG1 ensures that SMEs can effectively integrate these controls into their daily routines.

Evidence-Based

CIS Controls and Safeguards are based on industry recognized sources of breach data such as Verizon Data Breach, Incidents Report and Microsoft that provide a clear picture of the types of attacks and breaches being observed across the globe. These are mapped to the attack taxonomies developed by MITRE. The MITRE knowledge-base provides mitigations proven to be effective against its compendium of attack techniques. The CIS Safeguards map to attack mitigations from MITRE. This evidence based approach helps SMEs prioritize their security efforts, focusing on the measures that will have the greatest impact on their overall security posture.

This evidence-based foundation ensures that the recommended practices have been tested and proven to mitigate risks effectively. SMEs can implement these controls with confidence, knowing they are based on solid research and real-world success. The Essential Hygiene Safeguards protect against more than 80% of the attack techniques used by top attack types such as ransomware, system intrusions, and insider attacks.



Effectiveness of IG1 Against Top 5 Attacks (CIS Community Defense Model 2.0)

Community-Based

Developed and supported by a broad community of cybersecurity experts, CIS Controls benefit from continuous updates and improvements. This community-driven approach ensures that the controls remain current with emerging threats and best practices. SMEs can rely on the collective expertise of this community, knowing that the guidance they follow is informed by a wide range of industry professionals.

Compliance Frameworks Recognition

CIS Controls are mapped to compliance requirements from major security frameworks and standards such as NIST CSF, ISO 27001, SOC 2, HIPAA and PCI DSS. Essential cyber hygiene is the most foundational subset of these requirements. Achieving essential hygiene quickly and cost-effectively lowers the time and cost for achieving full compliance with the desired frameworks.

Prescriptive Approach

CIS IG1 offers a clear, prescriptive approach to cybersecurity. This structured approach provides SMEs with step-by-step instructions on how to protect their assets and respond to threats. By following this prescriptive guidance, SMEs can systematically improve their security posture and reduce their vulnerability to cyber-attacks.

Chapter 3

CIS IG1 Safeguards Explained

CIS Implementation Group 1 (IG1) represents the essential set of safeguards, serving as essential cyber hygiene within the broader framework of CIS's Implementation Groups (IG1,IG2 and IG3). Collectively, IG1, IG2, and IG3 encompass 153 safeguards distributed across 18 control groups. Specifically, IG1 includes 56 safeguards across 15 control groups.

While implementing every control within CIS's groups is important, Controls 13 (Network Monitoring and Defense), 16 (Application Software Security), and 18 (Penetration Testing) are exceptions. These controls extend into IG2 and IG3 and are designed to meet the advanced security needs of organizations based on their maturity, size, and resource availability. The remaining CIS controls, central to IG1, are crucial and should be prioritized. Let's delve into the 15 controls and 56 safeguards that form CIS IG1.

CIS Control 1: Inventory and Control of Enterprise Assets

Within CIS Control 1, IG1 includes two out of five safeguards:

1. Establish and Maintain a Comprehensive Enterprise Asset Inventory
2. Address Unauthorized Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 2 includes seven safeguards, with the first three essential for IG1:

3. Establish and Maintain an Up-to-Date Software Inventory
4. Ensure Authorized Software is Currently Supported
5. Address Unauthorized Software

CIS Control 3: Data Protection

CIS Control 3 emphasizes the necessity of a comprehensive data management and protection strategy, including six out of its fourteen safeguards as essential:

6. Establish and Maintain a Data Management Process
7. Establish and Maintain a Data Inventory
8. Configure Data Access Control Lists
9. Enforce Data Retention as Per Your Data Management Process
10. Securely Dispose of Data
11. Encrypt Data on End-User Devices

CIS Control 4: Secure Configuration of Enterprise Assets and Software

CIS Control 4 sets out best practices for maintaining the security configuration of hardware and software assets. Of the twelve safeguards, the first seven are included in IG1:

12. Establish and Maintain a Secure Configuration Process
13. Maintain Secure Configuration for Network Infrastructure.
14. Configure Automatic Session Locking
15. Implement and Manage Firewalls on Servers
16. Implement and Manage Firewalls on End-User Devices
17. Securely Manage Enterprise Software and Assets
18. Manage Default Accounts on Enterprise Software and Assets

CIS Control 5: Account Management

CIS Control 5 is dedicated to ensuring that all user, administrator, and service accounts within your organization are managed with precision and security. Within this control, four out of six safeguards are deemed essential:

19. Establish and Maintain a List of Accounts
20. Use Unique Passwords
21. Disable Dormant Accounts
22. Restrict Admin Privileges to Dedicated Admin Accounts

CIS Control 6: Access Control Management

CIS Control 6 establishes rigorous standards for the management and configuration of user access and permissions, incorporating five of its eight safeguards within IG1:

23. Establish an Access-Granting Process.
24. Establish an Access-Revoking Process
25. Require Multi-Factor Authentication (MFA) for Externally Exposed Accounts
26. Require MFA for Remote Network Access
27. Require MFA for Administrative Access

CIS Control 7: Continuous Vulnerability Management

CIS Control 7 is centered on the continuous identification, prioritization, documentation, and remediation of vulnerabilities within your IT infrastructure. This is increasingly crucial as cyber threats grow more sophisticated and frequent. Four of its seven safeguards are essential under IG1:

28. Establish and Maintain a Vulnerability Management Process
29. Establish and Maintain a Remediation Process
30. Perform Automated Operating System Patch Management
31. Perform Automated Application Patch Management

CIS Control 8: Audit Log Management

CIS Control 8 is instrumental in establishing procedures for collecting, alerting, reviewing, and retaining audit logs, which are crucial for detecting, understanding, and recovering from cyberattacks. Here are the essential safeguards associated with this control:

32. Establish and Maintain an Audit Log Management Process
33. Collect Audit Logs
34. Ensure Adequate Audit Log Storage

CIS Control 9: Email and Web Browser Protections

CIS Control 9 underscores the importance of securing email clients and web browsers, featuring seven safeguards, two of them being essential:

35. Ensure Only Fully Supported Email Clients and Browsers Are Used
36. Use Domain Name System (DNS) Filtering Services

CIS Control 10: Malware Defenses

CIS Control 10 details strategies to prevent and control the spread of malicious software across enterprise assets, highlighting three essential safeguards out of seven:

37. Deploy and Maintain Anti-Malware Software
38. Configure Automatic Anti-Malware Signature Updates
39. Disable Autorun and Auto-Play for Removable Media

CIS Control 11: Data Recovery

CIS Control 11 focuses on the critical need for data recovery and backup processes, with the first four of its five safeguards deemed essential:

40. Establish and Maintain a Data Recovery Process
41. Implement an Automated Backup Process
42. Protect Recovery Data
43. Establish and Maintain Isolated Copies of Backup Data

CIS Control 12: Network Infrastructure Management

CIS Control 12 establishes guidelines for effectively managing network devices to shield against exploits targeting vulnerable access points and network services. The primary and sole safeguard from this control in IG1 involves:

44. Maintain a Secure Network Architecture

CIS Control 14: Security Awareness and Skills Training

CIS Control 14 is dedicated to enhancing employees' cybersecurity awareness and skillsets, essential for the overall security posture of an organization. Regular training sessions and frequent refresh tests every 3–6 months are recommended to ensure employees are up to date with the latest security practices. Eight out of the nine safeguards from this control are deemed essential:

45. Establish and Maintain a Security Awareness Program
46. Train Workforce Members to Recognize Social Engineering Attacks
47. Train Workforce on Authentication Best Practices
48. Train Workforce on Data Handling Best Practices
49. Train Workforce on Causes of Unintentional Data Exposure
50. Train Workforce to Recognize and Report Security Incidents
51. Train Workforce on Managing Software Updates and Patches
52. Train Workforce on the Risks of Insecure Networks.

CIS Control 15: Service Provider Management

CIS Control 15 emphasizes the importance of meticulously managing service providers that handle sensitive data. This involves maintaining a robust evaluation system for these providers to ensure they meet stringent security standards. Only the first of the eight safeguards is considered essential.

53. Establish and Maintain a List of Service Providers

CIS Control 17: Incident Response Management

CIS Control 17 focuses on developing a resilient incident response capability to efficiently handle and mitigate the effects of security breaches. Three of the nine safeguards from this control are essential:

54. Designate Personnel to Manage Incident Handling
55. Establish and Maintain Contact Information for Reporting Security Incidents
56. Establish and Maintain an Enterprise Process for Reporting Incidents

Chapter 4

Challenges Faced by SMEs in Implementing CIS IG1

Although CIS IG1 safeguards are the least difficult to implement SMEs might still find them to be a handful. Despite the fundamental nature of these controls aimed at establishing essential cyber hygiene, several hurdles can impede effective implementation. These challenges primarily stem from the extensiveness of the safeguards, gaps in cybersecurity knowledge, and confusion over the selection of appropriate tools and services.

Overwhelming Volume of Safeguards

CIS IG1 consists of 56 safeguards, each crucial for fortifying an SME against common cyber threats. However, the sheer number of these safeguards can be overwhelming for small businesses, especially those with limited IT staff. This can result in a piecemeal approach leading to significant gaps in cybersecurity defenses.

Implementing the 56 CIS IG1 safeguards, done naively, could take as many as 16 tool types and the development of 10 processes and policies. This task presents a significant challenge for SMEs, primarily due to the wide range of available tools—from open-source solutions to advanced, high-cost options. The process of evaluating multiple vendors and selecting tools that best fit their specific needs can significantly delay implementation and introduce variability in costs. Furthermore, many SMEs may find themselves without the necessary expertise or resources to effectively develop and implement the required processes and policies.

Below is a detailed list of the 16 tool types and the 10 processes and policies essential for implementing the CIS IG1 safeguards.

Tools and Policies Needed

According to the CIS Controls Cost of Cyber Defense report, these controls are mapped over 16 tool categories and 10 policy categories to fulfill essential cyber hygiene requirements.

16 Tool Types

Enterprise and Software Asset Management, Service Provider Management, Data Management, Data Disposal, Encryption, Configuration Management, Firewall, Identity and Access Management, Password Management, Multi-Factor Authentication, Vulnerability/Patch Management, Log Management, Anti-Malware Software, DNS Service/Server, Data Backup and Recovery, Security Training and Awareness.

10 Policies/Processes/Plans

Enterprise Asset Management, Software Asset Management, Data Management, Secure Configuration, Account and Credential Management, Vulnerability/Patch Management, Log Management, Data Recovery, Security Training and Awareness, Incident Response Planning.

Lack of Cybersecurity Knowledge

Many SMEs do not possess in-house cybersecurity expertise. This lack of knowledge is a critical barrier when understanding the nuances associated with each safeguard. The technical nature of CIS controls requires a certain level of expertise to interpret and implement effectively.

Without this expertise, SMEs may struggle to fully comprehend the importance of each control and how it applies to their specific operational environment. Moreover, SMEs often underestimate the sophistication of potential cyber-attacks, which can lead to inadequate implementation of necessary safeguards.

Decision Paralysis and Tool Selection

Choosing the right tools and services to implement CIS controls is another significant challenge. The cybersecurity market is flooded with products, each claiming superiority over others. For SMEs, navigating this crowded space can be confusing. Decision paralysis can set in, stemming from uncertainty about which solutions are most suitable for their needs and budget. The fear of making the wrong investment can delay the implementation process, leaving businesses vulnerable to attacks longer than necessary.

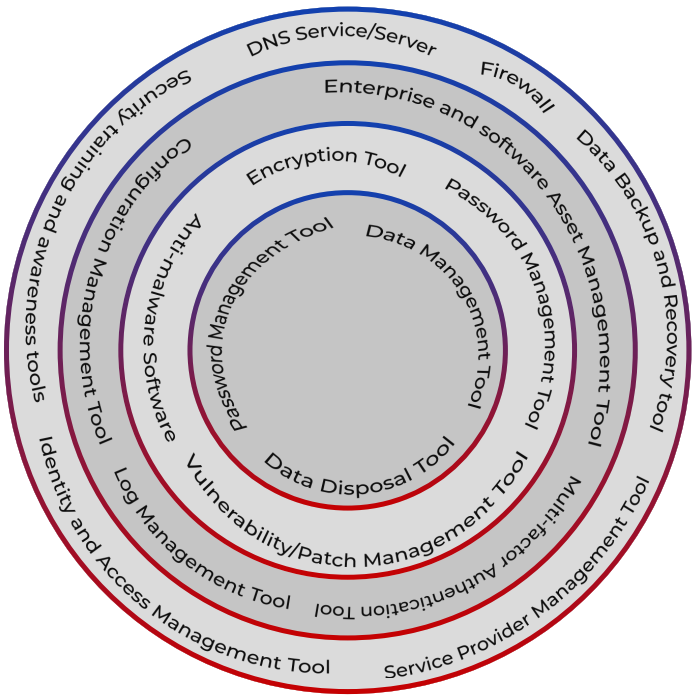
Furthermore, the cost associated with comprehensive cybersecurity tools can be prohibitive for SMEs. Balancing affordability with effectiveness is a fine line that many small businesses find difficult to walk. As a result, they might opt for less-than-optimal solutions that do not fully meet the requirements of CIS controls.

Role of Ebryx in Supporting CIS IG1 Implementation

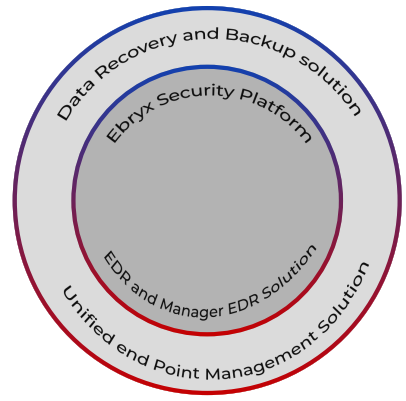
Ebryx understands the complexity and challenges SMEs face in implementing CIS IG1 safeguards. To address these issues, we have developed the Essential Cyber Hygiene Solution, which simplifies and consolidates the necessary tools and policies into an accessible and cost-effective package. Ebryx's Essential Cyber Hygiene Solution implements the 56 safeguards with a minimal set of versatile tools and 1 comprehensive service to build all processes and policies.

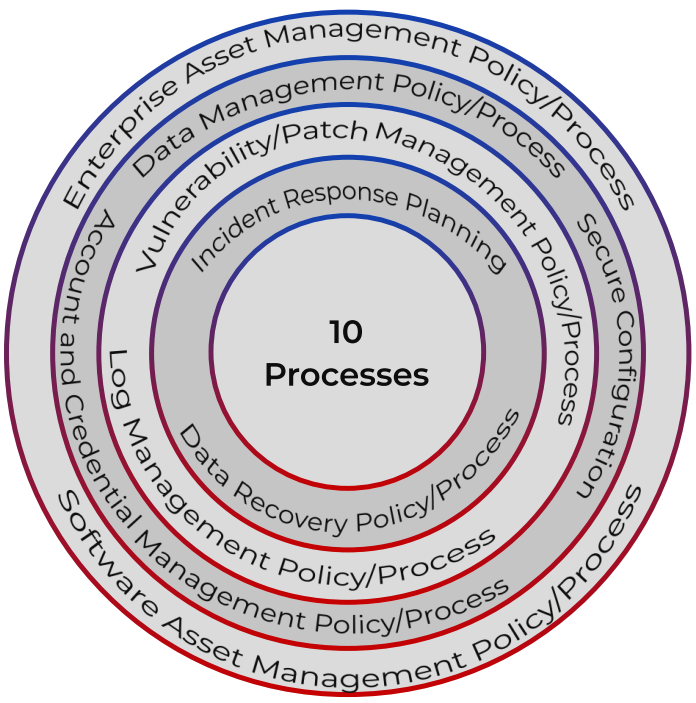
Simplified implementation of 56 CIS IG1 safeguards

Conventional way of implementing CIS IG1 controls



Reducing the number of tools required





Formulating the 10 processes/ policies with 1 comprehensive service

Ebryx Essential Cyber Hygiene Solution

Ebryx Essential Cyber Hygiene Solution establishes a solid security foundation for SMEs, shielding them from the most prevalent threats. This streamlined solution utilizes a carefully curated minimal set of versatile tools to implement all 56 CIS IG1 safeguards. Additionally, it consolidates the necessary 10 processes and policies into a single comprehensive service.

At its core, the solution comprises two essential tools coupled with Ebryx services, providing the fundamental security measures every SME should adopt. For those seeking more extensive protection, optional add-ons allow SMEs to fully leverage the entire suite of 56 CIS IG1 safeguards.

CORE OFFER

TOOLS

Ebryx Security Platform

A curated, minimalist set of innovative tools that Ebryx includes in its managed service.

Anti-Malware Solution

A selection of tools that do the job cost-effectively to state-of-the-art tools for the most sensitive organizations.

EBRYX SERVICES

Governance, Risk, and Compliance (GRC)

Comprehensive coverage of all required policies and procedures.

Security Awareness Trainings

Ensuring your team is well-equipped to recognize and respond to cybersecurity threats.

OPTIONAL ADD-ONS

Data Recovery and Backup Solution

Secure backup options and swift recovery capabilities.

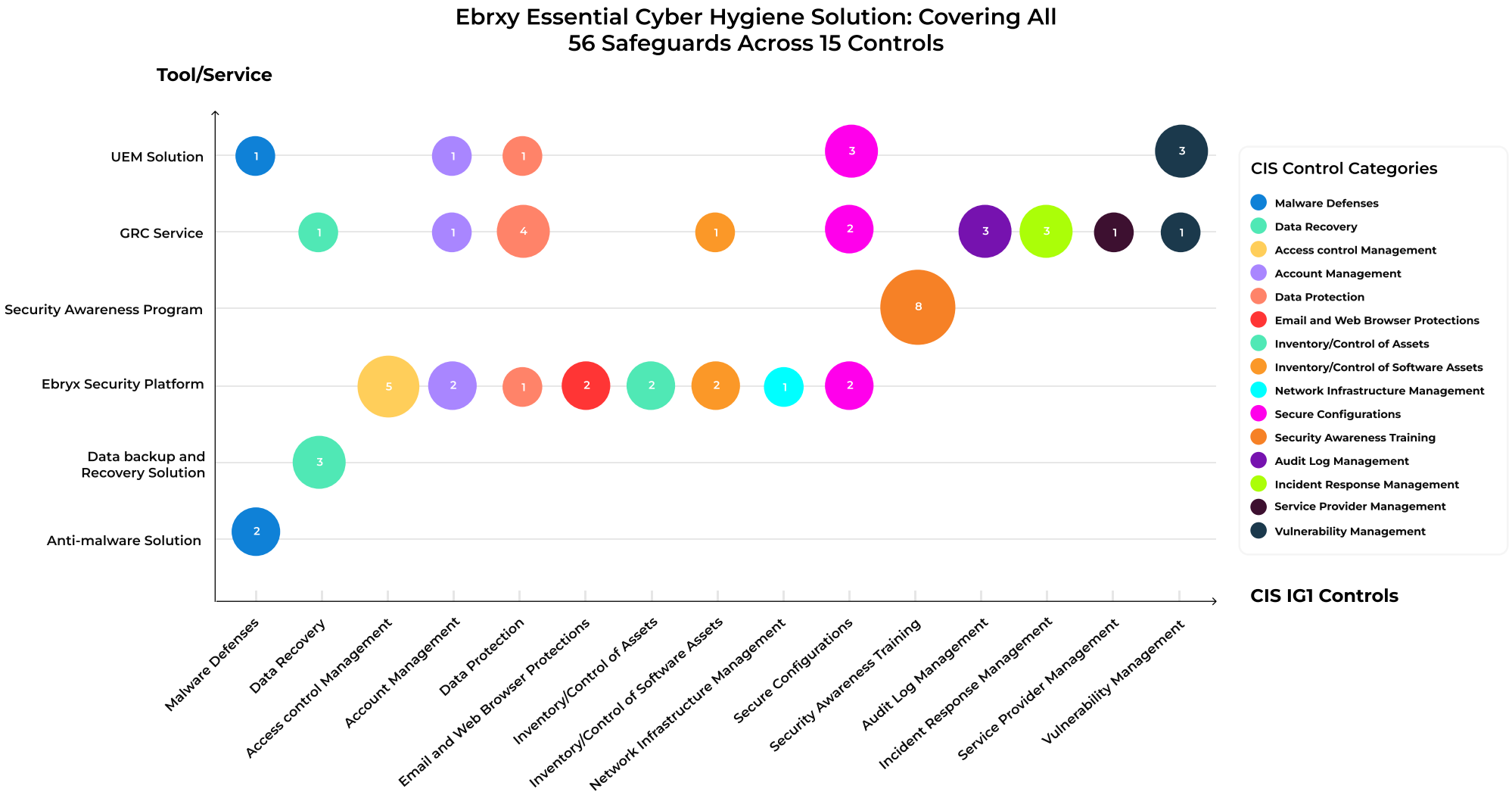
Unified Endpoint Management Solution

Centralized management of all endpoint devices to enhance security and compliance.

Simplifying Implementation

Our solution reduces the complexity of implementing CIS IG1 safeguards by reducing the number of tools required to implement the 56 safeguards and consolidating the 10 policy/process categories into one streamlined service package. This approach allows SMEs to implement the full range of CIS IG1 safeguards efficiently and effectively. The info graphic below illustrates the relationship between the tools and services within the Essential Cyber Hygiene solution and the 15 CIS IG1 controls. The size of each bubble indicates the number of safeguards (total of 56) each tool or service covers.

Click Here To Establish Essential Cyber Hygiene



Fill Your Essential Hygiene Gaps

An SME may have many essential safeguards implemented already and may have existing cybersecurity vendor relationships. Ebryx fills the existing gaps rather than replacing what an organization already has working well.

Beyond Essential Hygiene

Ebryx' Essential Hygiene solution has capabilities that exceed IG1 Safeguards. It provides coverage for several IG2 and IG3 Safeguards as well. In addition, Ebryx has an array of services such as SOC, pen-testing, DevSecOps and AppSec that cater to advanced security needs. For organizations with the most advanced security needs, we offer Zero Trust endpoint, network, application and data protection technologies and Zero Trust Architecture implementation services.

Conclusion

Recapping the critical role of CIS IG1, this eBook underscores its necessity for foundational cyber hygiene, setting a standard that effectively guards against prevalent cybersecurity threats. SMEs are encouraged to proactively enhance their IT security, aligning with CIS IG1 to fortify their defenses and mitigate potential vulnerabilities.

Ebryx has been at the forefront of delivering cutting-edge cybersecurity solutions for over a decade, protecting both SMEs and Fortune 500 companies. Our Essential Cyber Hygiene Solution is designed to make the implementation of CIS IG1 safeguards simple, cost-effective, and manageable. By leveraging our expertise and comprehensive security offerings, SMEs can achieve essential cyber hygiene and safeguard their operations against common threats with ease.

Choose Ebryx for a smarter, streamlined approach to cybersecurity. Our proven track record and dedication to excellence make us the ideal partner for your cyber security needs.

Establish Essential Cyber Hygiene Today

Links and Resources

- **Center of Internet Security:** https://www.cisecurity.org/
- **CIS Controls:** https://www.cisecurity.org/controls
- **CIS Community Defense Model 2.0:** CIS Community Defense Model 2.0
- **Microsoft:** Microsoft Digital Defense Report
- **Corvus Insurance:** Cover & Introduction - Cyber Risk Insight Index
- **CIS Cost of Cyber Defense:** https://www.cisecurity.org/insights/white-papers/the-cost-of-cyber-defense-cis-controls-ig1
- **Verizon 2023 Data Breach Investigations Report (DBIR)** - 2023 Data Breach Investigations Report (DBIR) (verizon.com)
- **Mastercard:** mastercard.us/content/dam/public/mastercardcom/na/us/en/smb/documents/mc-ovu-how-to-prevent-cyberattacks.pdf
- **Accenture:** State of Cybersecurity Report 2023 | Accenture

ebryx

ABOUT EBRYX

Ebryx offers comprehensive cybersecurity services for tech startups, SMEs, and Enterprises. We possess a unique combination of expertise in both technology research and operational security.

Our team holds certifications including GREM, GCFE, CEH, CISA, and CISSP. We also offer customized cybersecurity services based on client goals and threat landscape.

300+
Satisfied Customers

5+
Cybersecurity patents filed on behalf of customers

1 million+
Man - hours of security R&D

1000+
Successful security engagements