Managing SMB Cybersecurity Projects [1]

By Yogi Schulz

Do you think cybersecurity is expensive and consumes too much staff time? Do you believe your organization is too small, low profile and inconsequential to attract the attention of cyber attackers? Too many Small and Midsize Business (SMB) managers and owners may believe these misperceptions and sweep the topic of cybersecurity under the carpet at their peril.

What risks are we accepting by ignoring cybersecurity?

Cyberattacks include phishing attacks, data breaches, ransomware, theft of company intellectual property, corporate espionage, and identity theft. The adverse impacts of successful cyberattacks include:

- Reputational damage among customers and suppliers leading to loss of business.
- Financial losses due to the cost of repairing the computing infrastructure's damage and recreating data.
- Fines payable to regulators for violating the General Data Protection Regulation (GDPR) or similar regulations.
- Market share losses when theft of intellectual property creates competitors.
- Loss of revenue due to operational disruption.

Taken together, these likely impacts create a risk of bankruptcy.

Project managers too often fear cybersecurity projects because they feel daunting and technically complex. This article shows how a project that implements a subset of the CIS Critical Security Controls® (CIS Controls®) raises your SMB cybersecurity defences with low risk and excellent cost-effectiveness.

What is CIS?

The Center for Internet Security (CIS) is a non-profit organization founded in 2000. Its mission is to develop, promote and sustain best practices in cybersecurity to enable the Internet as a trusted environment. The members include government agencies, corporations and academic institutions. These members developed the CIS Controls® for computing environments by collaborating with experts in various disciplines, including security analysts, auditors, executives and policymakers.

[1] How to cite this article: Schulz, Y. (2024). Managing SMB Cybersecurity Projects, *PM World Journal*, Vol. XIII, Issue II, February.

Basing your SMB cybersecurity project on the CIS best practices, rather than developing your own practices, reduces project cost, risk and elapsed time.

What value do the CIS controls create?

The CIS community asserts that implementing the CIS controls:

- Prevents the vast majority of cyberattacks.
- Assures organizations that cybersecurity defences are comprehensive.
- Provides a framework for automating and managing cybersecurity defences well into the future.

Using the CIS controls framework to scope your SMB cybersecurity project provides the following project benefits:

- Quickly understand which cybersecurity risks are more critical and must be addressed first.
- Quickly builds a shared understanding of cybersecurity concepts and terminology among your project team.
- Leverages the expertise and experience of the global CIS community.
- Avoids the cost and delay of defining your own cybersecurity framework.
- Reduces the risk of missing cybersecurity risks in your own framework.
- Enables an independent assessment of your project work by the community of CIS consultants.

What are the CIS controls?

CIS defines 153 cyber defence safeguards grouped into 18 CIS controls. The safeguards are divided into three implementation groups (IG) as follows:

- IG1 – Implement essential cyber hygiene to thwart general attacks.
- IG2 – Manage complex IT infrastructure.
- IG3 – Secure confidential data to prevent sophisticated attacks.

The IGs recognize the resource constraints most SMBs operate with. To reduce cybersecurity risk, CIS recommends that SMBs focus resources first on the most straightforward and cheapest controls in IG1.

The IGs can quickly prioritize and sequence the contents of your project management plan. The IGs save time and cost while adding quality.

What differentiates the CIS controls from alternatives?

The CIS controls are an example of a governance, risk management, and compliance (GRC) standard. GRC standards describe cybersecurity best practices with their related processes and procedures. However, few GRC standards provide much detail on what is actually expected,

recommended or proven effective. The CIS controls' structure, description and organization address this shortcoming of other standards, making it easier and cheaper for SMBs to implement, operate and assess.

The CIS controls have proven their value by defining a base level of cybersecurity practices that SMBs can implement quickly and incorporate into their IT operations.

How do we begin?

Begin by downloading and reading the 4-page summary of the CIS Implementation Groups. This document helps you scope your project by illustrating how CIS divides cybersecurity into various topics and provides an overview of all the safeguards in the context of the control they belong to.

Then download the CIS Critical Security Controls® v8 Excel workbook. Reading the detailed descriptions of the many safeguards in the worksheet Controls V8 will give you a good understanding of the scope of the controls and how they are grouped.

This CIS information provides the core elements of your cybersecurity project charter and project management plan.

What's next?

Have your project team complete an assessment of CIS controls at your SMB. The assessment shows which cybersecurity controls are relevant to your organization, which are currently effective and which are not.

Your cybersecurity project is now ready to raise your cybersecurity defenses by remediating ineffective controls. Your project manager is now prepared to brief senior management and your board of directors about the following:

- The state of your cybersecurity defences.
- Your remediation project plan to raise cybersecurity defences.

These two points will give your SMB a high level of assurance that your cybersecurity risks are being comprehensively managed.

Continue your cybersecurity project by remediating the ineffective IG1 controls. Work on the ineffective IG2 and IG3 only if you need to reduce cybersecurity risks further. That's unlikely at an SMB.

As the project manager, you can reduce the cost and risk of a cybersecurity project at an SMB by basing it on the CIS Controls.

About the Author

Yogi Schulz

Calgary, Alberta, Canada

Yogi Schulz has over 40 years of Information Technology experience in various industries. Yogi works extensively in the petroleum industry to select and implement financial, production revenue accounting, land & contracts and geotechnical systems. He manages projects that arise from changes in business requirements, from the need to leverage technology opportunities and from mergers. His specialties include IT strategy, web strategy and systems project management.

Mr. Schulz regularly speaks to industry groups and writes a regular column for IT World Canada and for Engineering.com. He has written for Microsoft.com and the Calgary Herald. His writing focuses on project management and IT developments of interest to management. Mr. Schulz served as a member of the Board of Directors of the PPDM Association for twenty years until 2015. Learn more at https://www.corvelle.com/. He can be contacted at yogischulz@corvelle.com

His new book, co-authored by Jocelyn Schulz Lapointe, is "A Project Sponsor's Warp-Speed Guide: Improving Project Performance."