
Shields
Up
Cybersecurity
Project Management
Gregory J. Skulmoski, PhD

Shields Up

Shields Up

Cybersecurity Project Management

Gregory J. Skulmoski, PhD

Shields Up: Cybersecurity Project Management

Cover design by Gregory J. Skulmoski

Photo courtesy of pixabay.com/users/d0ran-18175716

Interior design by Exeter Premedia Services Private Ltd., Chennai, India

First published in 2022 by
Business Expert Press, LLC
222 East 46th Street, New York, NY 10017
www.businessexpertpress.com

ISBN-13: 978-1-63742-289-2 (paperback)
ISBN-13: 978-1-63742-290-8 (e-book)

Business Expert Press Portfolio and Project Management Collection

First edition: 2022

10 9 8 7 6 5 4 3 2 1

Description

We expect more automation, integration, and online activity in the foreseeable future, resulting in more cybersecurity risks and issues. Therefore, organizations and individuals are spending more resources on cybersecurity projects to implement, maintain, and optimize the confidentiality, integrity, and availability of their digital services and data. The demand for cybersecurity projects and expertise is growing and squeezing the supply of experienced cybersecurity implementers. That is, competent cybersecurity project managers will be progressively in high demand! The result is more cybersecurity technical experts (often in the junior ranks) will be asked to lead their first cybersecurity projects potentially before they are competent to do so; now what?

Shields Up: Cybersecurity Project Management is for our technical friends who are more familiar with Intrusion Detection and Protection Systems (IDPS) than risk registers but are now asked to lead cybersecurity projects. *Shields Up* provides an end-to-end project management framework tuned for cybersecurity projects. More experienced cybersecurity professionals will appreciate the innovative and lean elements of this approach. The reader is guided through the hybrid project management delivery approach and shown essential project management tools that increase the probability of project success.

Cybersecurity project management in *Shields Up* aligns with international standards such as the Guide to the Project Management Body of Knowledge, the National Institute of Standards and Technology Cybersecurity Framework, the ISO 27001 Information Security Management, and ISO 9000 Quality Management. A key feature of *Shields Up* is the reader can quickly apply the hybrid project management approach since it aligns with the global frameworks already followed by cybersecurity subject matter experts (SMEs) leading to more predictable and repeatable projects.

There are *microlearning* and *exercises* sections throughout the book to guide the reader to further learn about cybersecurity project management. Microlearning is an emerging way of continuous professional

development where the learner continuously learns in small chunks in addition to attending formal training opportunities like a three-day technology course. The book concludes with Appendixes including career planning tools to help the reader continue their professional development.

Keywords

cybersecurity; hybrid project management; NIST cybersecurity framework; ITIL 4 service management; Lean Six Sigma Optimization; risk management; certified information systems security professional; CISSP; continuous improvement; digital transformation; agile; career planning; lean management

Contents

Testimonials

Shields Up was reviewed by a heterogeneous group of diverse experts in technology, cybersecurity, and project management. The project management reviewers include both researchers and thought leaders in the project management specialty not only with decades of experience but also practicing as technology project managers. The cybersecurity reviewers are not typical book reviewers (e.g., academics); instead, these reviewers work in cybersecurity and related technical domains, resulting in a practical understanding of project management and cybersecurity. Therefore, these technology innovators know exactly the challenges and demands of cybersecurity projects and are well-placed to provide critical reviews such as the following:

"Must Read"

"Shields Up: Cybersecurity Project Management *is comprehensive and incredibly timely, given the ever-increasing cybersecurity threat landscape. It should be a must-read for all IT project managers because of the importance of ensuring that all IT projects clearly and deliberately address cyber risks as just a normal part of the process. You stated it perfectly when you wrote, 'It is good practice to build cybersecurity into our projects rather than adding cybersecurity as the project prepares to go-live.' The most important takeaway is the multitude of methodologies and frameworks that IT professionals look to for guidance can be nicely aligned and integrated into a coherent delivery model without compromising quality or efficiency. I must commend Greg on a well-written and comprehensive guide for tackling this new digital world we live in. Well done!"*—**Jason Roos, Chief Information Officer, King Abdullah University of Science and Technology, Saudi Arabia**

"Perfect Alignment"

"The book Shields Up: Cybersecurity Project Management *covers a broad spectrum of a reader's possible role within an IT department, especially in managing strategic and operational projects, including cybersecurity. The*

book will be appreciated by those who perform roles like project management, quality management, risk management, cybersecurity, IT operations support, strategic planning, and more. I was surprised to see its perfect alignment with NIST, ITIL, PMBOK® Guide, even ISO Risk Management. I advocate for a risk-based approach to managing cybersecurity, a central theme in Shields Up. *This book shares essential knowledge and expertise, and Greg nailed these and many more."*—**Irene Corpuz, PMP, ITIL, CISA, CEH, ISO 27001, Lead Implementer and Auditor, Manager—Projects, Federal Higher Education, United Arab Emirates**

"Outstanding Project Management Practice"

"Dr. Skulmoski's book is a metaphor for outstanding project management practice. It delivers content that's critical for the fast-developing business climate, and it does so with a precision of timeliness that is commendable. Shields Up *will prepare project managers to successfully deliver technology and cybersecurity projects."*—**Professor Alan Patching, PhD, Project Management, Associate Dean External Engagement, Bond University, Australia**

"Clearly and Succinctly Guides Cybersecurity Professionals"

"In Shields Up, *Skulmoski clearly and succinctly guides cybersecurity professionals on how to incorporate project management techniques and principles into their work to enhance both their projects and careers. He is clearly in tune with the struggles of cybersecurity professionals and the significant demands on their time. By providing expert advice on managing projects, which includes the latest thoughts and developments in the field, he gives cybersecurity professionals the critical tools they'll need to be successful."*—**Derek Molnar, PMP, IT Project Manager, Colorado State University, United States**

"A Solid Guide"

*"*Shields Up *is a solid guide covering all the stages and standards commonly found in cybersecurity projects, future demands, and a deep dive into why the IT delivery gap will only worsen due to skills shortage and increased demand for projects. The book perfectly covers standards, measurement practices (KPIs/SLAs), and guiding principles around cybersecurity project management from an end-to-end project perspective. Overall, the book richly describes the*

whole picture around technical project management at an enjoyable and great pace."—**Thiago Santos, Senior Technical Architect, Mulesoft, Canada**

"Pragmatic, Informative, and an Enjoyable Read"

"I begin by giving kudos to the author for writing this book. I found it very pragmatic, informative, and an enjoyable read. Shields *Up is well-structured and easy to read. The author provides a solid introduction to the cybersecurity and project management specialties supplemented with exercises and micro-learning opportunities. Additionally, I found the illustrations very helpful as they summarize the knowledge and aids learning retention, especially for each guiding framework (e.g., NIST, ITIL 4, and PMBOK® Guide).*

The book has the right balance between technical and project management content and is well suited for cybersecurity professionals and most technical roles. Shields Up *will also appeal to those who work in project management offices (PMOs).*

A vital benefit of this book is it can guide technical professionals to transition to a project management career. This book can be a quick reference guide to bridge the knowledge gap between technical and project management areas of practice. Overall, I enjoyed reading Shields Up *and recommend it to technical professionals interested in advancing their careers."*—**Israa Abulawi, BEng, ISACA, Enterprise Project Manager, Healthcare Care Technology and Data Management, United Arab Emirates**

"Unique Resource"

*"*Shields Up *is a truly unique resource. It explores the important domain of cybersecurity through a project management lens. I have not seen a book like this that is so comprehensive in scope and rich in advice while also being extremely practical. I believe this is mandatory reading for anyone wanting to make a career in our increasingly digital world of business transformation."*—**Professor Craig Langston, PhD, Project Management, Bond University, Australia**

Foreword

It was late July of 2012, and I had just landed in Abu Dhabi, having accepted a role with IBM in Middle East and Africa. I had been hired to set up and execute the learning function for a greenfield digital hospital, Cleveland Clinic Abu Dhabi. Recruited into IBM on the basis of my success implementing training programs for clinicians, I arrived at the temporary offices of Cleveland Clinic my first day of work sweating and jet-lagged, and met my key client, Dr. Gregory Skulmoski.

Greg was keen and cheerful, impeccably dressed, and energetic with a spring in his step. He greeted me enthusiastically. Though I already possessed almost 15 years of IT project management experience at that point, the subsequent weeks, months, and years working alongside Greg were an education. Some of my new colleagues loathed submitting deliverables (e.g., detailed requirements) to Greg as his reviews were exhaustive. Indeed, Greg insisted on the highest levels of quality, and in his exigence demonstrated deep familiarity with the theory and practice of project management.

I later learned that Greg's focus on quality assurance (preventing mistakes) rather than on quality control (fixing defects) was a team-building effort where the goal was to reinforce the *attention to details* skill and to get the technology right the first time, a very lean approach. Greg's teams delivered all their projects on time, and the go-live monitoring phase was exceptionally quiet indicating successful technology adoption. Greg's projects were closed out early because the new technology was predictable, reliable, and fit-for-purpose: technology characteristics that bring confidence to end users. When the project finished, vendors were able to cleanly depart because poor quality was never an issue; I appreciate that Greg took care of his vendors too.

Dr. Skulmoski also proved himself well-equipped and conversant in adult learning and training theory (andragogy), program and subject learning outcomes, instructional design, and many other components required for successful learning. Forward to March 2015, and we opened

the doors of Cleveland Clinic Abu Dhabi on time, and all caregivers could use the best-in-class systems to provide compassionate care. Greg would go on to accept a professorship at Bond University after a few years, and I subsequently carried forward what I learned working with Greg into a dozen other contexts in four countries, experimenting, relearning, yet much of the time standing on a foundation of certainties forged during my time working alongside Greg.

Throughout all these engagements I have participated in since leaving the site of Cleveland Clinic Abu Dhabi, several themes continue to emerge: How can project teams simultaneously combine the best of Agile and waterfall delivery methods? How can organizations address the "skills gap" in mission-critical fields such as cybersecurity? And how can large groups of clients and vendors come together to achieve results quickly and amicably?

In *Shields Up: Cybersecurity Project Management*, Greg artfully and scientifically cuts a path through the thicket of the contemporary project landscape, offering full-featured roadmaps to guide all those who might struggle with modern project management. But his treatment is more wide-ranging than just these areas. His framing and analyses of the current problems in business partner expectations, the pace of technological change, and the increasing importance of cybersecurity are all rock solid and extensively researched. He has also taken great care to engage his readers by creating exercises that will help them adapt their reading of this book and apply it to the cybersecurity project management conundrums they face today.

Shields Up is well-balanced, including meaningfully deep summaries of waterfall, Agile, and lean project management approaches, while keeping a pace crisp enough to prevent you from ever putting the book down. I found myself drawn to continue reading. Greg includes just the right amount of detail but includes numerous useful references, making it a suitable guide without ever becoming heavy reading.

Hybrid project management is a must-have ability in today's business environment, and Greg has elegantly detailed a flexible approach to mixing and matching the best of predictive and adaptive project management disciplines and allowing the reader to match techniques to suit the context of their own cybersecurity project.

For seasoned professionals in project management, *Shields Up* offers exceptionally clear and succinct explanations of critically important practices such as project initiation document structure, three-point estimation, risk and issue framework, and quality management. I found myself going back to review the text several times, capturing notes and slides, and then immediately putting many of Greg's hybrid project management practices into play in my latest project!

As you will observe in your reading of this work, *Shields Up* is lightweight and eminently practical. I find the approach refreshing and uplifting in its directness and simplicity. Like an authentically prepared "sugo" or a properly performed press-up, many of the fundamentals of project management are superficially understood by many yet poorly executed by most. Getting them right, while elusive, can mean obtaining extraordinarily results. In this book, Dr. Gregory Skulmoski presents you with tangible and effective methods to produce extraordinary results in your cybersecurity projects.

—Chris Walker, SHRM-SCP

Preface

Digital business transformation and emerging cyber-physical systems create unprecedented security risk

—Gartner 2020a, 1

Shields Up: Cybersecurity Project Management meets the demand for cybersecurity professionals to develop project management competencies to lead and succeed in their cybersecurity projects. Technology adoption and pervasiveness are increasing and perhaps accelerating, driven by Fourth Industrial Revolution innovations, and Covid-19 triggered digital transformation projects. *Shields Up* is designed to provide cybersecurity and other technology professionals a guide to plan, develop, manage, and implement cybersecurity projects.

Shields Up is divided into two parts: (i) Rising Demand for Technology and Cybersecurity and (ii) Hybrid Project Management. Part 1 frames project management in the context of an innovation delivery method; that is, to achieve strategic objectives, organizations increasingly initiate projects. The technology forecast is an increased demand for technology and cybersecurity. What is driving the demand for technology? What is the future foresight (examining possible future scenarios)?

Part 1: Increasing Demand for Cybersecurity Projects

Organizations that are agile and responsive to changing expectations and fleeting opportunities look to technology to gain a competitive advantage. They may implement technology to deliver new products and services or make processes more efficient by removing waste. By making processes lean and reducing materials or the time in the process, organizations attempt to satisfy customers. Satisfied customers purchase goods and services and make repeat purchases. Therefore, optimization and digitization are common business goals. Organizations also collaborate and connect people, systems, and data with technology; we see hyperconnectivity

increasing and extended digital ecosystems forming. Once digital transformation projects are implemented, organizations desire analytics-based decision-making capabilities; more technology projects with shortened delivery expectations are done right the first time!

In response to the increased demand for technology, organizations also see amplified demand for cybersecurity services ranging from protecting data assets to adding the new technology to the organization's threat monitoring systems. Business partners become collaborators in innovation, value cybersecurity services, and support increased cybersecurity budgets to secure their technology-driven innovations. However, with larger cybersecurity budgets, IT leadership is held accountable to meet business expectations. An issue facing the profession is a severe cybersecurity skills gap; organizations struggle to meet the demand for cybersecurity services due to a shortage of qualified cybersecurity professionals, including project managers. Many organizations have unfilled cybersecurity positions with long recruitment times. A consequence of these dynamics is cybersecurity professionals are asked to lead routine cybersecurity projects, leaving more complex cybersecurity projects for experienced project managers.

Organizations not only face challenges of implementing and managing more technologies, keeping systems and information secure, and completing work despite unfilled cybersecurity positions, they may also see more cybersecurity regulation. Governments and regulatory bodies are introducing cybersecurity regulations, and some organization are obligated to comply. Cybersecurity maturity models provide a pathway and guidance toward compliance and maturity targets, such as the Cybersecurity Capability Maturity Model (C2M2). Cybersecurity regulatory compliance drives more cybersecurity projects such as internal and external audits.

Organizations leverage cybersecurity and related standards and frameworks to fulfill cybersecurity expectations and requirements. There are two prominent cybersecurity standards to guide organizations to optimize their services: the Framework for Improving Critical Infrastructure Cybersecurity by the National Institute of Standards and Technology (NIST) and ISO 27001 Information Security Management (National Institute of Standards and Technology 2018, 1–55). IT departments may follow the Infrastructure Technology Information Library (ITIL)

standard to meet the demand for a service or product through planning, designing, developing, testing, implementing, operating, and optimizing phases to deliver value to the end user. While project management is explicitly embedded in ITIL, project management standards guide delivering value through a continuum of delivery approaches ranging from the predictive traditional (waterfall) project management delivery approach to adaptive agile techniques like Scrum and Kanban. The Guide to the Project Management Body of Knowledge (PMBOK® Guide) and PRINCE2 are two prominent project management standards supported with professional certifications. Central to cybersecurity, ITIL service management, and project management is quality management and the ISO 9001 quality management standard that guides organizations along a continuous improvement path.

Technology adoption is increasing at an accelerated rate due to many drivers such as artificial intelligence, the cloud, sensors, IoT devices, and the promise of technology-driven innovation. More technology results in increased demand for cybersecurity services. More regulation results in an increased demand for cybersecurity services. Increased demand translates into an increase in cybersecurity projects in an environment with a shortage of cybersecurity professionals and project managers. And hence, the purpose of *Shields Up: Cybersecurity Project Management* is to provide a proven method to plan, manage, and deliver cybersecurity projects aligned with leading global standards and best practices.

Part 2: Hybrid Project Management

The hybrid project management method is based on the traditional project management approach (predictive) with iterations where required. Hybrid project management draws on principles from the Agile Manifesto, the PMBOK® Guide, and other standards and frameworks. The project manager tailors principles, processes, tools, and methods suitable for the organization, project, and task. Tailoring can provide a lean project management delivery approach that facilitates the team being able to focus on producing products and services.

Most cybersecurity projects can be delivered with the traditional project management approach (initiate, plan, design, build, test, implement,

monitor/stabilize, and closeout) and traditional project management processes (e.g., quality and risk management). Hybrid project management utilizes traditional project management methods like scheduling, budgeting, and managing change. Innovative techniques are included in *Shields Up,* like Perfect-Likely-Outrageous (PLO, see *Project Schedule*) estimating and assessing your cybersecurity project with the Project Management Gizmo to develop a deep understanding of the project. Each cybersecurity project phase is tuned, a lean project management approach is described, and the processes, tools, and considerations are outlined.

Unfortunately, project failure is far too common in technology and cybersecurity projects. Project planning and risk management can improve the probability of project success. *Shields Up* outlines a lean planning process to deliver a project plan ready to take into the approval process. Even the best project plans can fail if risk management is poorly executed. Therefore, with quality management, risk management is at the heart of hybrid project management. Risk management need not be complicated with charts and statistical analyses; an intuitive qualitative risk management method often underlies successfully managing cybersecurity projects.

Supplemental material is included in *Shields Up* appendixes to take your learning further. The Project Management Gizmo tool helps assess your cybersecurity project and is included with permission from the International Project Management Association, presented in Rome, 2008. Any project can be assessed with the Gizmo to develop a comprehensive understanding of the project to begin the planning phase. When the Gizmo is used by the project manager, project sponsor, and team, a shared understanding of the project develops, and the probability of success improves.

A second appendix guides the reader to complete an iteration of career planning timed to coincide with an annual performance review. We are guided by best practices to continually improve not only systems but also our human resources. We also have a cybersecurity skills shortage. Therefore, the cybersecurity professional is encouraged to undertake career planning. *Shields Up* guides the reader through career planning steps to achieve career goals and build a sustainable career.

Finally, throughout the book, there are supplemental exercises and further guidance. *Shields Up* provides an approach to planning, managing, and delivering cybersecurity projects. The tools and practices can immediately be applied to your projects, and the exercises guide you to apply *Shields Up*. Many of the concepts outlined in this book can be supplemented with readily available online materials to extend your understanding of project management principles and theory. *Shields Up* provides microlearning opportunities in each chapter for the reader to increase their hybrid project management competence and success in projects.

Learning Outcomes

This book aims to provide an upskilling pathway for those interested in deepening their understanding of cybersecurity project management.[1] There are three learning outcomes for this book.

1. Apply hybrid project management to the increasing demand for more cybersecurity projects requiring formal project management competencies.
2. Implement cybersecurity project management aligned with global IT frameworks like NIST and ITIL.
3. Acquire and use hybrid project management principles and skills.

By reading this book and using it to plan and implement cybersecurity projects, the learner will better understand project management in the context of cybersecurity management and ultimately deliver successful cybersecurity projects.

---

[1] While *Shields Up* is focused on cybersecurity projects, the hybrid project management approach, processes and tools, can be applied to most technology and innovation projects such as automation, integration, and robotics projects.

Acknowledgments

I worked in Finance crunching numbers and one day my boss asked me to purchase twelve 386 CPU computers as part of the annual capital budgeting cycle: my first "IT project." Later, I participated in the selection team for a new financial system. We implemented a customized system that was late and over budget. I wanted to learn more about business to become better at projects, and I completed a traditional MBA. Even with this new business knowledge about labor law, return on investment calculations, and the four pillars of marketing, my projects continued to struggle. I searched for answers and discovered the project management specialty.

I enrolled in a project management program at the University of Calgary and learned how to plan and implement projects. I had many teachers who taught me the tools, processes, and finer points about project management. Thank you, professors Francis Hartman, George Jergeas, Janice Thomas, and Mr. Ken Hanley. All had practical project experience and helped me develop my own approach to managing projects. Dr. Francis Hartman led the project management specialization program and brought together engaged students to learn and have fun while polishing their assignments. Very quickly it seems that I almost finished my dissertation and thinking about what to do next? I spoke with Francis, and he recommended the Middle East. Shortly thereafter, I was hired by Zayed University in Abu Dhabi, United Arab Emirates, to teach project management.

I taught project management in the College of Information Technology for nine years and enjoyed academia and see our students learn and graduate. However, I yearned to practice what I professed; to manage my own projects. I joined Cleveland Clinic Abu Dhabi as a project manager near the beginning of the project and delivered 14 strategic projects ranging from technical (e.g., IoT/cloud technologies) to nontechnical projects (e.g., internal auditing). I worked in a PMO that followed leading standards such as ITIL, ISO 27000, ISO 9001, and the PMBOK®

Guide (more about these in Part 1). I experienced how multiple standards and frameworks can coexist to support delivering projects on time, on budget, and to the right levels of quality. I learned from my leadership (both technical and clinical), and I am grateful for the collegiality of my colleagues and team members. The tools, processes, and techniques in *Shields Up* were implemented and refined delivering projects at Cleveland Clinic Abu Dhabi. I was fortunate to win the 2017 Middle East Security Award, Chief Information Security Officers Council—*100 Rising Stars in Security and Risk* for how I managed risks in technology projects: hybrid project management works. After seven years of being on the sharp end of projects, I returned to academia and joined the project management program at Bond University, Australia.

I enjoyed being back in the classroom with diverse project experiences to share with our students. I joined a robust project management program with active and impactful researchers. My colleague Dr. Amir Ghanbaripour reviewed *Shields Up* and commented on the people aspect of projects: "The people who carry the shields are far more important than the shields (technology) themselves when it comes to cybersecurity." My students are also a source of influence: they graduate, work, and often contact me with their own stories of successfully applying the techniques in *Shields Up*. During this time, Dr. Kam Jugdev contacted me about writing a project management book for the Business Experts Press (BEP). We were PhD students at the University of Calgary and had previously published together. I teach a technology project management subject that includes unique content appearing in *Shields Up*. I am grateful to Dr. Jugdev and the BEP Collection Editor: Dr. Timothy Kloppenborg for their guidance. The BEP publications and Exeter Premedia Services team were skilled professionals who live and breathe lean project management to efficiently bring *Shields Up* to life. Thank you.

PART I

Increasing Demand for Cybersecurity

CHAPTER 1

Introduction

We live in extraordinary times; technological advances make headlines daily like "In the next decade, we'll experience more progress than in the last 100 years combined, as technology reshapes health and materials sciences, energy, transportation, and a wide range of other industries and domains" (Corbo and Ostojic 2021, 2). These technology promises are tempered with cyber-doom headlines like "Age of the cyber-attack: the US struggles to curb the rise of digital destabilization" (Rushe and Borger 2021, 1). To enjoy the benefits of transformative technologies, we need to keep these technologies and data safe to use. More technological adoption results in more cybersecurity projects. A project is "a temporary endeavor undertaken to create a unique product, service, or result. The temporary nature of projects indicates a beginning and an end to the project work or a phase of the project work" (PMI 2021, 28). Some organizations complete work through "initiatives" that are miniprojects with less complexity and risk (e.g., install an application patch). Technology professionals implementing initiatives can benefit from hybrid project management practices and tailoring; however, the focus in *Shields Up* is on more extensive and complex projects where project success is not easily guaranteed. But first, let's differentiate between projects and operations.

Projects Versus Operations

Information technology (IT) departments provide IT services like e-mail and business applications that cybersecurity teams keep safe and secure. End users leverage these services to complete their work to benefit their customers and organization; this is business operations. Service gaps and continuous improvement opportunities are identified, prioritized, and implemented as projects during business operations. Thus, projects feed into operations to help the business achieve its strategic objectives

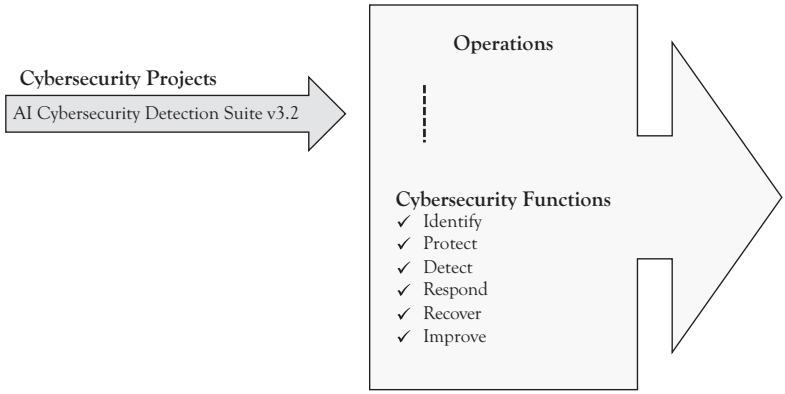

Figure 1.1 Projects deliver value to operations

(Figure 1.1). For example, IT provides cybersecurity services behind the scenes for most in the organization but are considered operations since we provide these services every day. We may encounter a problem that we need to rectify or identify an opportunity we wish to leverage; either can trigger a request for a new project. In Figure 1.1, we see that IT has identified an opportunity to improve threat detection functionality; they have approved and initiated a project to implement new detection software. By the length of the arrow, the project team is close to delivering the software into operations. We also notice the vertical dashed line in operations signifying a monitoring period after go live to fix any defects and optimize the new service.

We also implement projects for our business partners, such as upgrading our Enterprise Resource Planning (ERP) system or company website. Thus, we have operations and projects; we meet the needs of our stakeholders by initiating and delivering value into operations through projects. We follow the project management life cycle to deliver new IT services. Delivering new technical services using project management contributes to achieving business strategy (George 2008, 1).

The business initiates new projects for many reasons, such as responding to threats or vulnerabilities, taking advantage of an opportunity, increasing revenues, decreasing costs, or regulatory compliance, as we have seen. Typically, a new project request is sent to an entity with approval

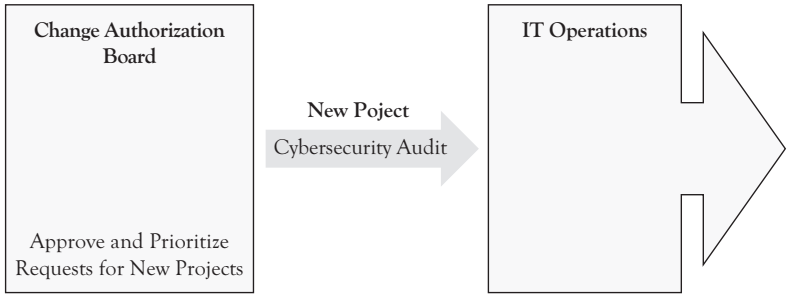

Figure 1.2 Change authorization board

authority like a change authorization board (Figure 1.2). A business case accompanies the request, and the proposed service and project is evaluated. The new project request may be approved, rejected, put on hold for future consideration, or require further information upon which a decision will be made. Some cybersecurity projects may be initiated through a formal committee, while others will be approved within the IT department. In Figure 1.2, the change authorization board has approved an internal cybersecurity audit to prepare for accreditation by an external agency.

Going through a formal change control process adds value for the organization:

1. Allow prioritization of requests for new IT services.
2. Contribute to meeting regulatory requirements.
3. Reduce the number of failed projects.
4. Better manage the flow of projects through the organization.
5. Improve our understanding of quality, time, scope, and time requirements for the project.
6. Provide a forum for businesses to propose new projects and services.

Some of the projects you will be asked to lead may come through a project prioritization and control process. We see organizations increasingly implementing more technology and cybersecurity projects using change authorization boards.

Technology Forecast: Change, Change, and More Projects

Working in the IT field, we see constant technological change. I am reminded that "change is certain in everything except vending machines"; soon, vending machines will become digital payment only. The changes underway are detailed in the *Fourth Industrial Revolution: World Economic Forum* where the researchers describe the Fourth Industrial Revolution as a digital revolution fusing digital, biological, and physical entities (Schwab 2016, 7). A distinguishing characteristic is the exponential speed at which these technologies emerge, bringing significant impact: "The scale of the impact and the speed of the changes taking place have made the transformation that is playing out so different from any other industrial revolution in human history" (Schwab 2016, 109). Data processing and communications are proceeding at ever-accelerating speed, which stresses data volumes, storage capacity, processing, and knowledge created (Creese, Saunders, Axon, and Dixon 2020, 10) and can trigger new projects (e.g., upgrade the infrastructure). We see some organizations embracing a continuous flow of digital transformation projects (Creese et al. 2020, 10), as seen in overall increases in IT budgets (Columbus 2020, 1).

We see people connecting with mobile technologies with unprecedented computing power, storage capacity, and functionality to access broad knowledge databases. Transformational technologies are emerging like artificial intelligence (AI), data modeling, 3D printing, nanomanufacturing, quantum computing, large-scale energy storage, and so forth. The popular literature trumpets the new age of digital acceleration and change (Table 1.1).

Our managers read these articles from digital thought leaders, expecting continued and accelerated technological advances. These bring digital opportunities to leverage and vulnerabilities to secure. These influential reports now drive business strategy, and new technologies change our customer expectations. These emerging technological promises are often translated into requests for new projects and secure systems. More cybersecurity projects are coming our way!

Table 1.1 Digital acceleration and change

Source	Message	Comment
McHugh (2020, 1)	"The pace of automation is accelerating, with more organizations creating fully automated value chains"	Now I have to worry about keeping our systems secure and the security of our partners' systems
Mulesoft (2020, 4)	"Organizations are increasingly investing in AI capabilities to expedite and personalize customer service, reduce human bias, and increase productivity"	These business requirements sound good, but that is a lot of technology to be secured!
Blackburn, LaBerge, O'Toole, and Schneider (2020, 3)	"Bold, tightly integrated digital strategies are the most effective approach to digital transformation"	Bold! I'm already working overtime to keep our data and systems safe and secure
Gonzalo, Harreis, Altable, and Villepelet (2020, 5)	"Companies must accelerate their online capabilities in both demand generation and operations management"	Accelerate? I already stated I am working overtime!
Skilton and Hovsepian (2018, 60)	"The near to longer-term impact of artificial intelligence and the fusion of intelligent systems into industries, individuals, and societies will have a profound impact on the role of the human at work and human experience"	I knew this 10 years ago! I live the profound impact systems have every day!
PMI (2018, 6)	A PMI report found 85% of the jobs that will be available by 2030 haven't even been invented yet!	I can barely keep current technologies safe, let alone technologies required to support jobs that don't yet exist
Scheibenreif and Raskino (2021, 1)	"Machine customers represent the biggest new growth opportunity of the decade. In fact, by 2030, at least 25% of all purchasing decisions will be delegated to machines"	Now, I need to think about machines being hacked, resulting in machine customers illegally using our credit cards!

Disruptive Technologies Acceleration

Innovation and technology adoption is accelerating, and there is a feeling that if organizations do not implement a digital transformation strategy, it may be too late for laggards to catch up to technology early adopters (Aaldering and Song 2021, 12). Indeed, Covid-19 triggered a massive acceleration of digitization (Scholtz 2021, 2). These technologies need to be secured as they can present new vulnerabilities. However, as the pace of technology adoption accelerates, so will the need to secure technologies also accelerate. Thus, early adopters will likely continue to implement technology at an accelerated pace, and laggards will try to catch up. The result will be more technology projects and more cybersecurity work at an accelerated cadence.

New Technologies to Protect

The specific technologies and trends are less important here; the general trends related to technology adoption are of greater interest. We see the rollout of 5G technologies leading to a new era of connectivity, complexity, and opportunity for organizations and bad actors. The World Economic Forum (Creese et al. 2020, 6) predicts the following transformative technologies will be increasingly important: ubiquitous connectivity, AI and machine learning, quantum computing and next-generation identify, and access management. Combining technologies like IoT and sensors will bring new opportunities and assets to protect. Organizations will increasingly move components of their technology ecosystem to the cloud, thereby adding additional complexity to cybersecurity efforts.

We can expect transformative change with next-generation computing like computational collaboration, distributed computing, and quantum computing resulting in increased computing speed and efficiency. Early adopters will have a disruptive advantage and can transform strategy, operations, supply chains, and markets (Corbo and Ostojic 2021, 2). It is no surprise that our organizations have early adopters who will propose new technologies to help us innovate. Expect more proposals that include AI technologies. However, these emerging technologies change the risk equation with increased and evolving threats, widening attacks,

continued structural weaknesses, and grave consequences due to cyberattacks (Creese et al. 2020, 13).

AI Technologies Become Mainstream

AI is the next big thing (PMI 2019, 2). We see AI early adopters in several industries, including advertising, automotive, banking, electronics, financial services, health care, insurance, media, pharmaceuticals, telecommunications, and transportation (Corbo and Ostojic 2021, 2). We can expect AI to be widely applied to:

1. Automation and productivity improvements across the value chain;
2. Next-generation customer experience;
3. Transformation in research and product development;
4. New business models, products, and services (Corbo and Ostojic 2021, 2).

Therefore, we will see more AI-related projects implementing applied AI applications and services. These AI-supported applications and services will need cybersecurity involvement.

We can expect the emergence of IoT to grow and accelerate as equipment vendors stay connected to their devices in the field to predict maintenance requirements using AI (Dahlqvist, Patel, Rajko, and Shulman 2019, 3). The technological advances in sensor technologies and the adoption of smart cities are also driving IoT adoption (Dahlqvist et al. 2019, 3). We may see nano IoT sensors attached to the human body, ingested, or integrated with organs to allow human body monitoring and augmentation (Skilton and Hovsepian 2018, 30). Innovations like ingested IoT sensors are examples of the rapidly growing IoT technology segment. Indeed, we may see as many as 50 billion IoT devices by 2022, and such "rapid proliferation has made these products appealing targets for a growing number of cyberattacks" (Microsoft 2020, 30). Again, there are more opportunities for cybersecurity services delivered through projects.

Unfortunately, bad actors will increasingly use AI and associated technologies in their cyberattacks. For example, the malicious use of AI will become more sophisticated and pervasive, where automating attacks can

see increases to attack speed and scale (Creese et al. 2020, 28). Adversarial machine learning (actions to attack machine learning) is predicted to grow (Microsoft 2020, 35). The attackers will be able to extract more value from stolen data and will be able to deliver more damage from their attacks (Creese et al. 2020, 12). Offensive AI will find new ways of attacking its targets. AI defenses will also see an increase in adoption by organizations and individuals. AI defense capabilities will see an improving defense posture, dynamic threat detection, proactive defense, increased speed in response and recovery, and improvements to attack determination (Creese et al. 2020, 29). AI will help us detect threats in languages we do not understand and find and understand malicious patterns that no human would ever consider (CyberEdge Group, LLC 2020, 34). "We might even go out on a limb and say that machine learning and other AI technologies offer our last chance to catch up with and overtake the bad guys" (CyberEdge Group, LLC 2020, 35). More cybersecurity projects are predicted.

Shields Up

Cybersecurity Project Management

Gregory J. Skulmoski

The demand for cybersecurity expertise is growing phenomenally; enhancing cybersecurity project skills will boost technology professionals' careers and improve organizational cybersecurity readiness.

Shields Up: Cybersecurity Project Management provides an end-to-end framework tuned for cybersecurity projects. More experienced cybersecurity professionals will appreciate the innovative and lean elements of this approach. The reader is guided through the delivery, management, and optimization approach that increases the probability of cybersecurity project success.

Cybersecurity project management in *Shields Up* brings together international frameworks such as the Guide to the Project Management Body of Knowledge, the National Institute of Standards and Technology Cybersecurity Framework, ITIL 4 Service Management, the ISO 27001 Information Security Management, ISO 31000 Risk Management, and ISO 9000 Quality Management. A key benefit of this book is the reader can quickly apply the hybrid project management approach since it combines global frameworks already followed by cybersecurity professionals leading to successful projects. **Never before has cybersecurity project management been so important.**

Gregory J. Skulmoski, BEd, MBA, PhD, CITP, FBCS, is a seasoned (and bruised!) project manager who has led technical and non-technical projects in Australia, the Middle East, and Canada, with about $10 billion project experience. He is a Certified Information Technology Professional and a Lifetime Fellow of the British Computer Society.

Dr Skulmoski teaches project innovation management at Bond University. Greg's teaching focus is on practical processes and tools to successfully implement, manage, and optimize technology. Greg used the hybrid project management approach to win the Chief Information Security Officers 2017 Middle East Security Award. Dr Skulmoski brings experience, theory, standards, and practice together in his book *Shields Up: Cybersecurity Project Management* to successfully deliver cybersecurity projects.

Portfolio and Project Management Collection

Timothy J. Kloppenborg and Kam Jugdev, *Editors*

ISBN: 978-1-63742-289-2

BEP BUSINESS EXPERT PRESS

Leader in applied, concise business books