CHAPTER 10

Create Your Rational Cybersecurity Success Plan

This has been *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. I've made this guidance as detailed and specific as possible because all too often, we get only platitudes or generalizations on the topic. We can't afford that anymore. Misalignment between security and the business has a corrosive effect on any security effort it touches. And as organizations transform into digital businesses, they fall under increasing IT-related risk and regulation. Aligning security to business leaders and business processes is exponentially more important now.

In this final chapter, let's go through what we've covered in the book and help you complete a Rational Cybersecurity Success Plan Worksheet[1] to record your progress pursuing cybersecurity-business alignment.

The Success Plan uses a simple methodology with just a few steps:

1. Scope out priority focus areas.
2. Make a quick assessment of your current state.
3. Identify stakeholders (in security-related business roles).
4. Define improvement objectives (within your priority focus areas).
5. Identify metrics.
6. Track progress.

[1] "Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_10

The priority focus areas, or priorities, always refer to the six Rational Cybersecurity Pareto Priority areas described in Chapter 1 and throughout the book.

Action: *Don't skip this chapter!* Even if you're an extremely busy CISO it will be worth your while to work through these exercises (or delegate them to a trusted staff member and monitor the learnings and improvement opportunities).

Print out or open a copy of the Success Plan Worksheet to edit online as you go through Chapter 10.

Note If you have already filled in parts of the worksheet during earlier chapters, use this chapter to recheck or complete your work on steps 1–4, then proceed to steps 5 and 6.

10.1 Scope Out Your Priority Focus Areas

Not all readers head up the whole security program. Not all CISOs or security leaders have the same starting point or wish to work on all the priority focus areas simultaneously. Starting where you are, here's how to calibrate the scope of your Success Plan. New CISOs or CISOs with a mandate to expand or reshape the security program should consider acting on all six Rational Cybersecurity priorities. Other security leaders – such as well-established CISOs just wanting to tweak their program, part-time interim CISO caretakers, or security managers under the CISO – should primarily focus on the priorities within their own area of responsibilities or where they see the greatest gaps and opportunities.

Action: Check mark your priority focus areas in Table 1, Section 1, of the Success Plan Worksheet.

10.2 Identify Stakeholders

Chapter 2's section "Clarify Security-Related Business Roles" and Table 2-2 contain a list of typical stakeholder roles. In a small business, some of the roles may not exist and others will be combined in a few people. In a large business, multiple people may fill some of the same roles across business units. Prioritize relationships with all stakeholders or just with the ones covering your priority focus areas.

Action: Fill in the name of the person holding each role identified in Table 2 of Section 2 in the worksheet. If a role doesn't exist or is called something else at your organization, then remove, edit, or annotate the rows in Table 2 as necessary. In the Contact Plan

column, note whether the person should be contacted now or later and who will be the relationship manager (i.e., you or someone else from the security team). Fill in the Notes column with any known projects, issues, or pain points to cover with the stakeholder.

10.3 Make a Quick Assessment of Current State

The following exercise doesn't replace a more in-depth, formal assessment, but it can help set quick, actionable improvement objectives.

Make a quick assessment of the current state of security practice for each of your priority focus areas. **Base the scoring criteria for each area on how you'd answer the majority of the questions for it provided in the following "Sample Criteria to Consider During Scoring":** Strong "no" (1=strongly disagree), qualified "no" (2=disagree), a balance of "yes, no, maybes" (3=neutral), qualified "yes" (4=agree), or strong "yes" (5=strongly agree).

If you can't provide an educated guess at the 1–5 rating for an area, leave it blank and proceed to the next exercise. You'll be able to come back and finish this once you've had more time to think about it and/or talk with specialists or stakeholders. Also, if you're actively working on improving security practices and business alignment in a focus area, return to the worksheet to make changes in your assessment at later milestones (3 months or 6 months).

Action: Mark the scores from 1 to 5 for each row in Table 3 of Section 3 in the worksheet corresponding to your priority focus areas. Record any notes about your assessment score for each priority focus area in Table 4. Be brutally honest – no one has to see this except you.

Sample Criteria to Consider During Scoring for each focus area:

Develop and Govern a Healthy Security Culture:

Security governance:

1. Does the security governance structure align well with the way IT and the business are organized?
2. Is the business's definition of security (mission, structure, and operating principles) captured in the security charter, and is it reflective of the way the business really works?
3. Does a security steering committee meet regularly; do security, IT, corporate administration, and LOB representatives with signing authority regularly attend it; and is it effective at addressing cross-functional security issues and moving security projects forward?

4. Does a risk management forum exist and does it hold business risk owners accountable for risks and serve as a useful venue for reviewing top risk analyses and treatment recommendations?
5. Are security policies, standards, processes, and procedures generally up to date and do day-to-day practices in the business generally follow them?
6. Is the security budget centralized, or are multiple security budgets rationalized in the sense that relatively little overlap exists?

Security culture:

1. Do business executives prioritize and support cybersecurity (i.e., consider it strategic)?
2. Do business, IT, and development managers provide resources to security projects and help enforce security policies?
3. Do security team members have positive relationships and communications with business stakeholders?
4. Does the CISO treat communicating with IT and business leaders as being a top priority?
5. Are security leaders incentivized to
    a. Maintain regular communication with IT and business leaders in their functional area?
    b. Improve their communication skills and those of their team members?
6. Does the security organization have a user awareness function sized to the business?
7. Does the user awareness and training function
    a. Communicate in an efficacious manner ("we can do this," "here's how others have been [safe, successful]")?
    b. Target awareness programs to specific audiences?
    c. Coordinate programs with the audiences' leadership?
    d. Provide role-specific training?

e. Recruit champions among the target audiences and "train the trainers"?

f. Provide information or free tools that will help staff and their families improve cybersecurity at home?

g. Coordinate with the marketing organization's internal communications program?

h. Use innovative and entertaining communications mediums, products, or services?

8. Does the security leadership or awareness program itself measure whether awareness and training programs are improving

   a. Security-related behavior?

   b. Attitudes and perceptions about the security program?

   c. Understanding of policies, tools, and procedures (cognition and compliance)?

   d. Compliance audit results?

Manage Risk in the Language of Business:

1. Are business owners held accountable for information risk?
2. Are business, IT, and security teams using consistent terminology for discussing risk and consistent criteria for assessing risk?
3. Are stakeholders coming to security for guidance or advice before taking important decisions that could create risk?
4. Are risk assessments used to prioritize security projects, manage third parties, or make other decisions?
5. Is a quantitative risk analysis methodology in use?
6. Are issues, risks, exceptions/acceptances, and top risks monitored in an issue management system; IT governance, risk, and compliance (IT GRC) tool; and/or risk register?
7. Are top information risks being regularly communicated to executives and the Board, and is the dialogue constructive?

Establish a Control Baseline:

1. Does the business have a "control framework" and/or a "control baseline" document that lists the control objectives for IT and the business?
2. Does the security organization have published guidance mapping the control objectives to the required control activities for different levels of risk or different situations (e.g., data classifications, use of third-party services)?
3. Is the control baseline mapped to requirements documents and solution architectures for critical operational systems in IT and security environments?
4. Is the control baseline updated and followed?
5. Do IT, security, or third-party management groups have a shared responsibility framework to aid in evaluating third-party services?
6. Does an architecture document specify how the controls should be deployed?
7. Does the business have an assurance or an audit function to verify controls are operating?

Simplify and Rationalize IT and Security:

1. Does the business have a simplified and rationalized IT environment?
2. Is there a published, up-to-date IT strategy?
3. Has the security strategy aligned to the IT strategy?
4. Is the business use of a hybrid multicloud environment governed well?
5. Does IT publish a service catalog and are security services included in it?
6. Does the security organization work closely with third-party management to assess third-party risk early in the commercial evaluation process?

7. Is the security organization working with DevOps teams to develop DevSecOps processes?

Control Access Without Creating a Drag on the Business:

1. Does the business have a cross-functional identity and access management (IAM) team?
2. Does the IAM team report to or coordinate with security?
3. Does the business have coherent access policy models (roles, rules, and groups) in key IT environments?
4. Can IAM systems quickly enable new digital relationships for new applications or business partners?
5. Does the business have someone working on data governance?
6. Does the business have a Chief Privacy Officer or a Data Protection Officer?
7. Are data stewards, or data owners, assigned for sensitive or business-critical information?
8. Does the security department know where all the sensitive data is stored?
9. Are privileged access rights (i.e., root account or domain administrator) restricted to small groups of users?
10. Is privileged access controlled or monitored?

Institute Resilient Detection, Response, and Recovery:

1. Does the business have
    a. Log standards?
    b. A security operations center (SOC) and/or an MSSP?
    c. A security information and event management system (SIEM)?
    d. A Computer Security Incident Response Team (CSIRT)?

2. Does the business have incident response plans and playbooks?
    a. Have these plans and playbooks been proven effective in real incidents or tests?
3. Does the business have an asset inventory and a current business impact assessment (BIA) identifying critical assets?
4. Does the business have a business continuity and disaster recovery (BC/DR) plan and program?
5. Has the BC/DR plan been tested?

10.4 Identify Improvement Objectives

Consider each of the Rational Cybersecurity priorities you've selected or all of them. Define one to three improvement objectives for each priority and enter them into the Identify Improvement Objectives table row for each priority. As much as possible, emphasize quick-hitting improvement objectives to keep this effort fluid, maintain momentum, and expose problem areas sooner.

The following subsections provide some example improvement objectives for each priority focus area. The reader can consider the examples, but understand they are only a few of many possible areas to improve.

In general, the examples focus on improving the kinds of issues a security organization with low maturity in the Focus Area could have. They also emphasize work that can be done in alignment with stakeholders outside the security organization.

Choose improvement objectives that fit the business's current gaps, maturity level, and priorities. It should be possible to accomplish each objective in the short term (less than 90 days). If necessary, break critical but large improvement objectives down into smaller chunks.

10.4.1 Develop and Govern a Healthy Security Culture

Action: If "Develop and Govern a Healthy Security Culture" is one of the selected priority focus areas, note improvement objectives in Section 4, Tables 5a and 5b, of the worksheet. Use the examples in this section to help choose three to six improvement objectives based on Chapters 3 and 4.

Security governance:

- Create or revisit the security charter and work on getting business buy-in for a definition of security that is fully aligned with the business needs.
- Review Chapter 2's Table 2-2 listing security-related business roles to find any that seem appropriate for a business like yours but aren't being fulfilled. Communicate with stakeholders and find out the reason.
- Plan for a security policy refresh and identify business stakeholders affected by the current policy documents and potential new ones.
- Review the minutes or records from the last 6–12 months of security steering committee (or other coordinating group) meetings, review its strengths and weaknesses, and propose improvements.
- Work with the business finance office to collect information on all security budgets, sources of funding, and funded project charters. Call out any obvious gaps or overlaps.

Security culture:

- Continuously maintain the worksheet stakeholder engagement information in Table 2.
- Assess your communication style or habits and improve at least one practice.
- Get the security team to assess group communication styles or habits and improve at least one practice.
- Create and manage at least one practice for user awareness and training improvement (e.g., task key team members to collect feedback from one to three business or IT stakeholders on security-related communications).
- Prepare an informal briefing on security culture (using this chapter as a resource) and present or discuss it with at least one of your business or IT executive sponsors.

10.4.2 Manage Risk in the Language of Business

Action: If "Manage Risk in the Language of Business" is one of the selected priority focus areas, note improvement objectives in Section 4, Table 6, of the worksheet. Use the guidance and examples in this section to help choose one to three improvement objectives based on Chapter 5.

If the business doesn't yet have a formal information risk management program, look for improvement objectives in section "Establish the Context for the Risk Program." For example:

- Perform a PESTLE analysis[4] to understand and document the risk program's business context and discuss it with at least one business or IT executive sponsor.
- Task security and risk team members unfamiliar with FAIR to read section "Open Factor Analysis of Information Risk (FAIR)" and the Open Group Standard: Risk Analysis (O-RA)[7] and other FAIR resources.[2]

To improve a risk management program that's up and running, consider the following sample improvement objective:

- Review the organization's asset inventory program and identify an IT champion willing to work with the risk management function on devising a method to capture asset risk scores and risk metadata as described in section "Implement Asset Risk Profiling."

To improve identification of top information risk at the executive level, consider the following sample improvement objective:

- Meet with executive stakeholder(s) responsible for reporting risk to an Audit Committee (or other risk management forums). Identify or discuss
  - Who are, or could be, accountable risk owners for categories of information risks
  - Potential overlaps between information risks and top enterprise risk scenarios

[2] "FAIR Resources," Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/RiskManagementResources

Readers seeking more assistance or guidance on building a risk program can contact us via our website (https://security-architect.com/contact-us) or visit our risk management resources page.[3]

10.4.3 Establish a Control Baseline

Action: If "Establish a Control Baseline" is one of your priority focus areas, note improvement objectives in Section 4, Table 7, of the worksheet. Use the guidance and examples in this section to help choose one to three improvement objectives.

As you'll recall, the purpose of a control baseline is to create the minimum viable list of controls from the security control domains that apply to the business, map the controls to the business IT environments, and develop applicability guidelines for them. From Chapter 6's section "Address Common Challenges," however, we found many issues and gaps in the way businesses typically address controls. The following are suggestions for quick-hitting improvement objectives:

- Evaluate the current control baseline document(s) to see if they can be used as is or as a draft starting point.

If the business requires a new or rewritten control baseline:

- Create an initial detailed outline for a new control baseline using a spreadsheet or a governance, risk, and compliance (GRC) tool. Populate the draft using information from the 20 security control domains in Chapter 6.

If a current and credible security assessment is not available:

- Perform a rapid enterprise risk assessment based on the methodology from Chapter 5, section "Perform Enterprise Risk Assessments to Identify Top Risk Scenarios," using available data to identify at least a rough list of top information risks.

[3] "Risk Management Program Review," Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/RiskManagementResources

- Perform a control gap assessment against the control baseline and the list of top information risks. Depending on the size of the business, rapid or deep security assessments[4] can be performed within a 30-60-90-day period.

Note A good security assessment is a control assessment aligned to a list of top information risks.

10.4.4 Simplify and Rationalize IT and Security

Action: If "Simplify and Rationalize IT and Security" is one of your priority focus areas, note improvement objectives in Section 4, Table 8, of the worksheet. Use the guidance in this section to help choose one to three improvement objectives based on Chapter 7.

Understand that a secure digital business must be one that continually plans, curates, and aligns IT capabilities in a defensible architecture. From Chapter 7's section "Address Common Challenges," however, we found many issues with technical debt, lack of IT strategy, and difficulty keeping pace with LOB requirements and shadow IT. The following are some example improvement objectives:

- Locate document(s) labeled as an "IT Strategy" or serving that purpose. Provide security organization commentary on them and discuss with the IT stakeholders. Align them with the current security project portfolio or road map as appropriate.
- Help the IT organization operate in the "IT-as-broker" mode by collecting information on cloud-based security services options (e.g., vulnerability scanning, multifactor authentication, etc.) it could provide or encouraging adoption of services already provided.
- Analyze development tool chains in use and discuss potential DevSecOps solutions with development managers.

[4] "Security Assessments," Security Architects, LLC, May 2020, accessed at: https://security-architect.com/SecurityAssessmentResources

Evaluate the opportunity to set up Security Championship Program(s) in IT. Discuss the idea with senior IT managers that might support the idea and/or identify staff members in IT that might be good candidates in championship roles.

10.4.5 Control Access with Minimal Drag on the Business

Action: If "Control Access with Minimal Drag on the Business" is one of your priority focus areas, note improvement objectives in Section 4, Table 9, of the worksheet. Use the guidance and examples in this section to help choose one to three improvement objectives based on Chapter 8.

Access control and data governance are critical for enabling digital businesses to use applications and tools productively, to form new digital relationships with customers and other external parties, and to stay in compliance with regulations. From Chapter 8's section "Address Common Challenges," however, we found many IAM infrastructures are outdated, IAM and data governance processes are immature, and IAM teams lack cross-functional buy-in.

Of all the Rational Cybersecurity priorities (with the possible exception of risk management), IAM and data governance are the most complex ones.

- Conduct a rapid security assessment focused on IAM and data governance[5]; together they constitute a large and critical piece of the security program.
- Identify quick-hitting IAM improvement projects. Use the business impact assessment (BIA), the enterprise risk map, or other sources to find critical assets and risk owners; map the IAM and data governance control baseline (per Chapter 8, Table 8-1) against the assets and connect with one to three stakeholders to learn their IAM and data governance pain points.

[5]"IAM Assessments," Security Architects, LLC, May 2020, accessed at: https://security-architect.com/IAMResources

If you are the CISO (or "Head of Security") but the IAM team reports to another organization and isn't closely aligned to security:

- Strengthen the dotted-line reporting relationship of the IAM team to security. To do this, work with the CIO or other higher executive functions over IAM.

10.4.6 Institute Resilient Detection, Response, and Recovery

Action: If "Institute Resilient Detection, Response, and Recovery" is one of your priority focus areas, note improvement objectives in Section 4, Table 10, of the worksheet. Use the guidance in this section to help choose one to three improvement objectives based on Chapter 9.

As we discussed in Chapter 9, section "Business Unpreparedness for Incident Response and Recovery," businesses in 2020 will continue to face an elevated threat environment. Due to unpreparedness or immaturity as well as "Lack of Visibility or Access to All IT Systems," IT and security leaders may not have their defensive priorities clearly focused on critical systems. It's inevitable that "Protect" controls will sometimes fail.

The following are examples of cyber-resilience improvement objectives:

- Review contingency plans for incident response for the business's top risk scenarios or critical assets. Identify and list which are missing. If none are complete, develop a detailed outline for at least one plan and discuss it with affected stakeholders.
- Review incident response policies and procedures with affected stakeholders to ensure they are up to date and still agreed on.
- Review BC/DR plans with affected stakeholders to ensure they are up to date and still agreed on.

10.5 Specify Metrics

Some improvement objectives are one-time projects. But others require recurring activities or processes.

Note any ongoing improvement objective whose progress you'd like to track in the Specify Metrics in Table 11, Section 5, of the worksheet. For each, list one to three top metrics. I filled in examples for the "Increase CISO and security team communication with stakeholders" objective:

- #Stakeholder 1 on 1 meetings
- #Stakeholder team briefings

"Cybersecurity is a contact sport."

Craig Callé, CEO at Source Callé, LLC

10.6 Track Progress

Action: For each priority focus area where you have improvement objectives

- Use Section 3's Tables 3 and 4 to update your quick assessment ratings of the priority focus areas at the 30, 60, and 90 days' marks.
- Use Section 5's Table 11 in the worksheet to track your progress with each of your identified improvement objectives' metrics.

10.7 This Is Not the End

Cybersecurity-business alignment is an ongoing effort. We do it because security is an inherently cross-functional activity. Per Chapter 7, Harvard Business Review research found that 75% of cross-functional teams are dysfunctional, but that projects with strong governance support have a 76% success rate. The cross-functional challenges – and the potentially disastrous consequences of business *disengagement* – are why security leaders should prize alignment so highly and constantly work to make it happen.

But maybe you finished the book and wonder, what now? Hopefully not, because if you took the opportunity to work through the Success Plan, you'll have written down some action items. I've concluded the book in an actionable manner precisely so you wouldn't have put it down with that "So what?" feeling.

We have much to do just to accomplish the six Rational Cybersecurity priorities. That's why the Success Plan encourages setting quick-hitting improvement objectives and provides a framework to track progress. Don't try to boil the ocean with your first Rational Cybersecurity Success Plan; make it an iterative process. If you stick with it, you'll still be here 90 days from now moving forward with cybersecurity-business alignment. Step by step. "Baby steps can take us up Mount Everest," as my life coach likes to say.

You'll want to continue taking action after 90 days, setting successively more impactful improvement objectives.

Meanwhile, I'm hoping that the work of Rational Cybersecurity continues to evolve. Together, we can create additional iterations of the guidance in the "Define Rational Cybersecurity Improvement Objectives." In the published edition you've just read, I've assumed we're just getting started and suggested very basic improvement objectives. But I have to believe that – if security leaders focus on cybersecurity-business alignment – our capabilities will mature significantly and improve business's cybersecurity outcomes. If we reach the point where the example improvement objectives in this chapter seem like baby steps and more advanced ideas online take them up a few levels, we will have succeeded.

There is a great opportunity for the security leader with strong communication skills and an understanding of what's needed to make cybersecurity more strategic to the business and better aligned with stakeholders. Be that leader. You don't have to do it alone. Engage your staff in the vision of a Rational Cybersecurity program. Engage with a community of others in a journey of continuous learning about how we can become more effective at aligning and running our cross-functional projects.

10.8 This Is the Beginning of an Open Information Flow

Rational Cybersecurity for Business has been released via Open Access under the Creative Commons license so that we can create an open information flow to fully use and build on this material. As readers, you can continue to evolve the work. You can take pieces of this material, improve it, and please do share it (with attribution) for the rest of us. And, since good reviews are invaluable to help a book be found by potential readers, please review it on Amazon and/or your preferred social media outlet.

The journey of this book doesn't end with publication, it begins. I will be doing more in the coming months and years to connect us. For now, here's how we can connect.

Connect with me on LinkedIn: www.linkedin.com/in/dan-blum-author-architect/

Join the LinkedIn Security Architecture Group: www.linkedin.com/groups/3394596/

Follow me on Twitter: Daniel Blum @RationalCybrSec

Subscribe to the Security-Architect.com blog

Check the links included in the book

https://security-architect.com/SuccessPlanWorksheet

https://security-architect.com/RiskManagementResources

https://security-architect.com/IAMResources

https://security-architect.com/SecurityAssessmentResources
