Setting Your Roadmap to Success

Information Security Leaders: Communicate the Value of Your Program

> "TrustMAPP meaningfully communicates the state of information security and risk to all levels within an enterprise. It customizes the presentation of the same data so the message is readily understandable and actionable by O&T teams, up to the C-suite and the Board. It is a product that I wish was available when I was the CISO at Citi."
> – Steve Katz – Board Executive Advisor Deloitte &
> Former CISO of Kaiser Permanente and Citi Group

Introduction

Cybersecurity is finally getting the attention it deserves. From the boardroom to the C-suite, top executives are not only asking for regular cybersecurity updates, they're also asking better questions. Yet, while security leaders are enjoying this newfound attention to security, this shift in focus means security leaders need to devote more of their limited time to assess and communicate the effectiveness of their organization's security program.

Demonstrating alignment to strategic business objectives and ensuring security resources are deployed in the right way has also received increased focus. All these increased corporate needs translate into the security leader spending large swaths of time translating highly technical metrics into executive-level dashboards, and mapping how security operations enable and protect the organization's strategy and business objectives. We offer a picture of an easier way.

How Do You Spend Your Time? What Else Could You Be Doing?

While most security leaders are thankful to finally have a seat at the table, many report being frustrated at the amount of time they and their teams are spending to prepare reports and provide updates. According to executive advisors CEB[1], security leaders often spend three to four weeks to prepare for their next presentation to executives and boards. This adds up to as much as 15 to 20% of CISO's and their team's time per year. With a shortage of cybersecurity talent in the marketplace (read, understaffed cybersecurity teams), more efficient reporting is needed.

[1] 5 Myths About Presenting to the Board of Directors on Cybersecurity https://www.cebglobal.com/blogs/5-myths-about-presenting-to-the-board-of-directors-on-cybersecurity/

Wish #1 – A platform to save time on reporting

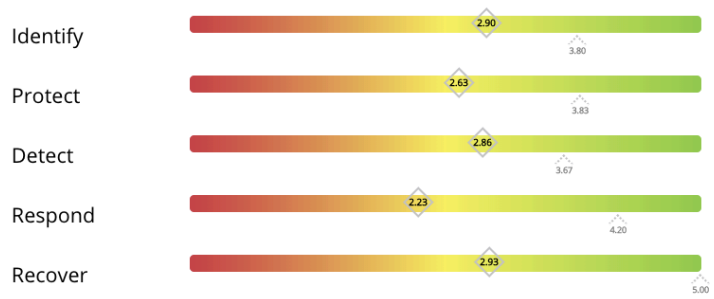

Figure 1 - Clear & Simple Dashboards for Different Audiences

These staff time investment estimates are driven by manually translating technical metrics and other key performance indicators from a wide array of information security tools deployed throughout the modern organization. These tools provide an abundance of technical security data that, while useful to security leaders and their teams, don't translate well into an effective security narrative for the C-suite or the boardroom. The security leader is left having to manually thread disparate security details together into a compelling story for the top leadership. A herculean task.

Security leaders who have adopted TrustMAPP® reported that a key benefit of the platform was its ability to save time when compared to manually-produced reports and spreadsheets. In addition, TrustMAPP leverages a familiar business language — maturity — to measure the business value of security.

Tracking Trends Over Time — How Are We Doing?

Aggregating key operational metrics from technical controls provides a foundation for the conversation. The key to ***reporting the right information, in the right context, at the right time*** is building the narrative to assess and communicate, at a strategic level, the performance of the various security-related activities/projects. To accomplish this security leaders must focus on security processes that map to controls they are monitoring.

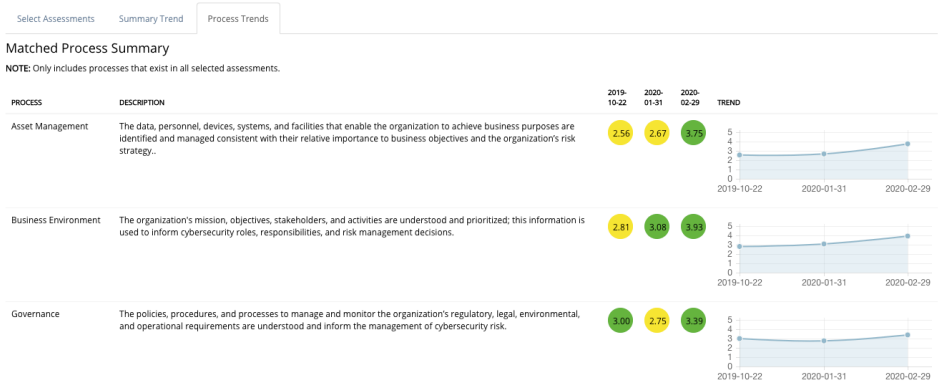

Figure 2 Trending analysis to compare performance

Processes are how TrustMAPP assesses and manages the capabilities of your security program. To this end, we've coined the phrase "controls are for auditors, processes are for managers." All controls managed by a security team are aligned to common processes. This reduces the overhead of reporting and builds consistent KPIs for the team. Instead of managing 500 to 1,000 controls, a team can report on the performance of 20 to 40 processes – both easier for security leaders to communicate, ***and*** for business leaders to grasp.

Wish #2 – Platform to easily track and report trends across time

The ability to report on how your organization has fared over time across various business processes is key to having engaged conversations with top leadership. However, without the support of a tool, security leaders are faced with having to manually correlate points in time across various metrics.

Maturity — One Measure to Rule Them All

Over the past decade, the cybersecurity industry has coalesced around using maturity to manage, measure, improve and communicate security program capacity[2]. The benefits of using maturity to measuring, reporting, and goal-setting is its broad use and applicability to the entire umbrella of cybersecurity activities (people, process and technology) within the organization.

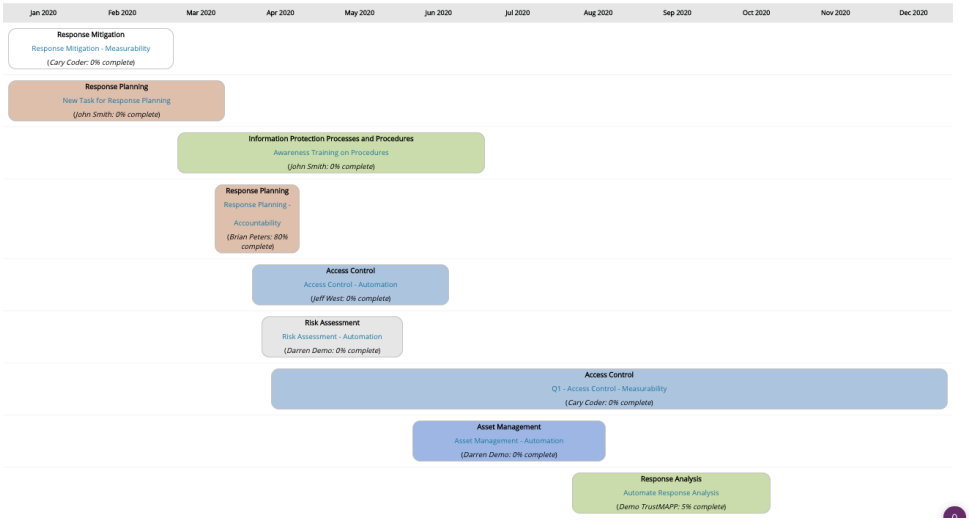

Figure 3 Dynamic task creation for roadmap development

Wish #3 – Platform to provide a sound approach to measuring and managing security activities

Maturity assessments form the basis by which security leaders can measure the effectiveness of the organization's cybersecurity capability. When aggregated across the organization's security processes, the maturity measures provide a unique security profile of the organization. With maturity-based assessments, security leaders have a sound metric by which they can measure, report, and track the performance of various businesses processes.

With a maturity based approach, security leaders can clearly express key points they need to provide top leadership, go over the decisions that need to be taken, and ensure that top leadership has the information they need to make the best decision.

How Do We Plan for the Future?

By assessing the maturity of one's processes — or groups of controls organized across lines of business or across general categories of controls (e.g., authentication or incident response) — security leaders can easily thread a narrative. The narrative will not only allow them to communicate the state of cybersecurity in the

[2] TrustMAPP — Maturity Assessment, Profile, and Plan: A MAPP to Clearer Information Security https://trustmapp.com/executive-reporting/

organization, but also create — together with top leadership — profiles of where the organization should be, in terms of performance, in the next quarter, the next year, or the next three years.

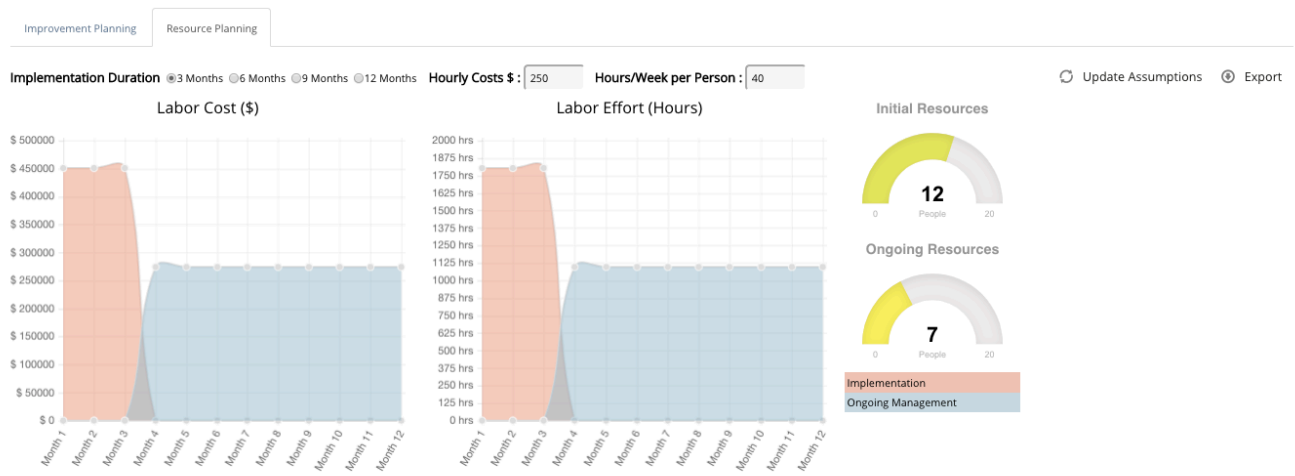

Figure 4 Security program improvement forecasting based on time and cost

Wish #4 – Platform to provide both assessment and planning capabilities

Presented with clear information about the maturity of the various security processes, the security leader and management can go over the gap between current and desired maturity levels and determine if the organization is performing at the level that it should be. When the program is falling short, appropriate remediation efforts can be planned and appropriately funded when management understands the maturity gaps and where and why planned resources will be spent.

Challenged to find a new way to communicate the effectiveness of his cybersecurity program to the board, the CISO of a mid-sized software firm shifted the focus away from security controls and began using the language of process maturity, enabled by TrustMAPP.

By aligning maturity scoring with organizational objectives, the CISO breathed new life into monthly boardroom presentations. Using the TrustMAPP platform to bridge the operational and strategic aspects of cybersecurity management, the CISO can now demonstrate the measurable value of the firm's investment in security-focused tools and resources.

Board members are pleased with these changes. Today, regular updates about program maturity helps inform strategic decision-making and improves members' understanding the benefits of adopting effective security processes.

How does Security Performance Align with Our Risks?

Security leaders talk about the importance of combining both maturity and risk to provide a complete story. Too often risk is given in board rooms without context on the level of effort and money saved or additional monies required to achieve specific goals. The full picture given to the executive leadership team or board of directors must be both a risk posture and a maturity posture. Otherwise we are communicating as leaders only half of the story. Risk provides insight on weakness and probability of weakness materializing. Maturity provides insight into current capabilities to manage and mitigate risks and lends intelligence to forecasting resource and investment plans for future improvement of identified weaknesses. With TrustMAPP teams can align business objectives to security processes to risk categories and determine plans for improvements.

How Does TrustMAPP Empower the Security Leader?

TrustMAPP is a platform that can perform and track maturity measurements for your program's security processes along with desired maturity goals, generate various profile views, and provide cost estimates for closing the maturity gaps. TrustMAPP provides a configurable dashboard, enabling security leaders to generate reports for various audiences including boards, management, peers, or internal audit.

Using TrustMAPP Internally — Benefits for the Security Department

With TrustMAPP, security leaders can improve their ability to track and manage security activities under their control:

- Determine the strength of current security processes
- Track maturity trends between processes and across time
- Estimate cost and effort levels to achieve desired maturity levels
- Plan and forecast remediation
- Update executive leadership on progress

Using TrustMAPP Externally — An Executive Communication Platform

When it comes to having improved interactions with the board and the C-suite, TrustMAPP empowers the security leader to:

- Provide effective communications/reporting throughout the organization
- Strengthen the support and trust from executive leadership and stakeholders
- Engage with top leadership to improve cyber risk governance including overall strategy and processes

Up and Running in Days

Most TrustMAPP deployments can be completed in just a few days, including framework selection — since most standard frameworks are already supported — customization, and initial test-run. Putting TrustMAPP to use is as easy as 1, 2, 3:

1. **Assess maturity** – Survey templates pre-configured with the NIST Cyber Security Framework and ISO27001, as well as industry-specific regulations such as HIPAA, PCI DSS, FFIEC, FISMA, and CMMC, to provide assessment questions to functional owners of key processes.
2. **Profile results** – The COBIT maturity model is built-in to find gaps and see overall security and compliance program posture, with results returned in a clear dashboard summary.
3. **Plan objectives** – Priorities for improvement are ranked by business impact and cost-analyzed for one-time and ongoing investment needs, to provide sound strategic and budgetary planning.

TrustMAPP Features

- An easy-to use interface.
- A 50+ built-in template frameworks and regulations, including NIST CSF, NIST 800-53, ISO27001, CIS Top 20, GDPR, HIPAA, PCI DSS, FFIEC CAT, NY DFS, and many other combinations that enable expert information security assessments in just days. An analytics engine turns responses into scores for each process or control across maturity measured on a scale of 1 through 5.
- Reported time savings of 70-80% compared to a manual approach.
- Visual reports that turn assessment results into clearly ranked priorities.
- Ability to set a desired maturity goal for security processes and then calculate related cost estimates to address gaps.

Conclusion

TrustMAPP empowers the security leader with a clear picture of the organization's security posture, including trending analysis, planning and budgeting, and built-in support for multiple frameworks. With TrustMAPP's cloud-based platform, you can score, track, and report on the maturity of security processes within weeks, instead of months, using the platform's built-in dashboards. TrustMAPP helps security leaders create and communicate an information security roadmap to guide the organization's security activities.

About TrustMAPP

TrustMAPP delivers continuous Security Performance Management, giving CISOs a real-time view of their cybersecurity maturity. TrustMAPP tells you where you are, where you're going, and what it will take to get there.

From a single source of data, an organization's security posture is visible based on stakeholder perspective: CISO, C-Suite, and Board. TrustMAPP gives organizations the ability to manage security as a business, quantifying and prioritizing remediation actions and costs.

TrustMAPP aligns engagements to business objectives by providing information security management and governance, enterprise risk and compliance, and data privacy. We partner with business leaders to bridge the gap between operations and business management. Our proprietary methodology titled MAPP provides a maturity-based approach to cybersecurity program management.

TrustMAPP's key difference is a focus on maturing business processes – rather than short-range audit controls. Maturity-based security management is becoming best practice in our industry, and TrustMAPP is leading the way.

> The CISOs who can align their risk metrics with the business's most pressing issues are more likely to be heard by strategic leadership. Making these insights easy to consume through intuitive dashboards can only help further solidify the CISOs' importance. — Deloitte[3]

[3] Deloitte The new CISO: Leading the strategic security organization https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html