esm
The Strategy Execution Company

A Guide To

Building a Winning Cybersecurity Program

Part 1 Planning Your Cybersecurity Strategy

www.esmgrp.com

Introduction

The intent of this three-part series, **"A Guide for Building a Winning Cybersecurity Program,"** is to provide today's IT Security Leaders with insights and considerations for building a winning cybersecurity program that aligns with organizational business drivers.

Part 1 provides insights into planning the program strategy. **Part 2** addresses tactical considerations; while **Part 3** focuses on managing and executing the cybersecurity program.

Underlying this three-part series is the recognition that Cybersecurity programs are not a one-size fits all undertaking. Each organization differs in their risk profile, business constraints, and investment appetite.

Overview

Cyber risk exists where threats, vulnerabilities and the organization's attack surface (i.e. assets and information) intersect. The goals of an organization's cybersecurity program are to minimize the probability of such threats from exploiting organizational vulnerabilities—and to reduce financial and reputational impact from the loss of use, or value of assets and information. The cybersecurity program capabilities are designed to protect and keep watch over an organization's intangible and tangible assets—or the risk landscape. Some common components comprising this risk landscape include:

- Cyber assets (networks, applications and devices)
- Data (personal, customer, partner, supplier, etc.)
- Intellectual property
- Non-IT related equipment
- People
- Property and facilities
- Supply chain
- Third-party providers

How do today's IT Security Leaders adapt their cybersecurity program strategies to protect their organizations from this constantly changing risk landscape?

In 2020, the role of Information Technology (IT) security leaders like the CIO, CISO or CTO will continue to expand into executive management leadership. The IT strategy no longer is a linear, siloed business function. Rather, digital transformation, high-speed mobile networking, and the potential capabilities of next-horizon technologies like Artificial Intelligence (AI), Machine Learning (ML), and Quantum computing are compelling IT security leaders, executive management, and lines of businesses (LOBs) to rethink how they can use

technology, processes and people to transform business performance and the customer experience.

Business models are now being optimized to take advantage of these disruptive technologies and their capabilities. At the same time, this optimization of the business strategy is driving the IT strategy to find new ways to use emerging technologies to create new and transformational revenue streams. What does this mean for IT security leaders?

Part 1

Planning Your Cybersecurity Strategy

> *Findings from the recent IDG's, State of the CIO, 2020" survey indicate that 95% of CIOs see their role as expanding beyond traditional responsibilities into other areas. The top five areas that CIOs reported to be involved in from a leadership capacity includes: cybersecurity (64%), data privacy / compliance (49%), customer experience (49%), operations (36%), and business development (36%).*

While the survey shows that cybersecurity and data privacy/compliance remain a chief concern, it also points to this shift in the CIO's role from just implementing technology to a cross-functional leadership capacity. A critical success factor for today's IT security leaders will be the adoption of robust, cross-functional governance in their cybersecurity program that balances the growing importance of enterprise data strategy with changing legal and regulatory statutes, rising security threats, risk tolerance, and privacy-aware consumers.

How can IT security leaders build, execute and evolve a comprehensive cybersecurity program that aligns with their business objectives? The purpose of this three-part white paper series is to guide IT security leaders through a checklist of better practices for building or restructuring a successful cybersecurity program.

PRACTICE 1: Align the Cybersecurity Program with your Organization's Strategy and Goals

Using the analogy of the IT security leader as an architect, consider this initial process as building the foundation for cross-functional governance into the cybersecurity program.

Cybersecurity programs are complex with interdependent defensive capabilities. Following are preparatory steps that help articulate the vision of the program at completion, and validate alignment with business goals in concrete, tangible ways.

Step One: Align cybersecurity program capabilities with the needs of the business. This step ensures that you have a clear understanding of the current state capabilities of the cybersecurity program from a business view to answer the question, *why are we doing this?* Rather than implementing the newest technology or trying the "latest" widget, instead what needs be addressed here are the requirements and concerns of the organization's users from their business perspective. Taking a cross-functional view, consider what the cybersecurity program needs to accomplish and establish a timeline for achieving those objectives. For example, ask:

- What are the short-, intermediate-, and long-term goals of the cybersecurity program?
- And, what capabilities need to be in place to achieve these goals?
- What must be protected? What are the "crown jewels" of the organization?
- What are the most pressing risks facing the organization? And, how might these threats impact the organization's bottom line?
- What basic functionality should the cybersecurity program include?
- What is envisioned for current- and future state usability? How to achieve the delicate balance between accessibility and protection to ensure an undue burden is not put on users while providing adequate measures to protect the organization?
- How can operations be improved to consistently maintain and improve the organization's security posture?
- How can funds optimally be deployed to protect the organization?

Addressing the business view is where the cybersecurity program gets aligned with key business drivers. This alignment enables buy-in from all stakeholders by creating a financial understanding of investments across all cybersecurity domains also addressing the allocation

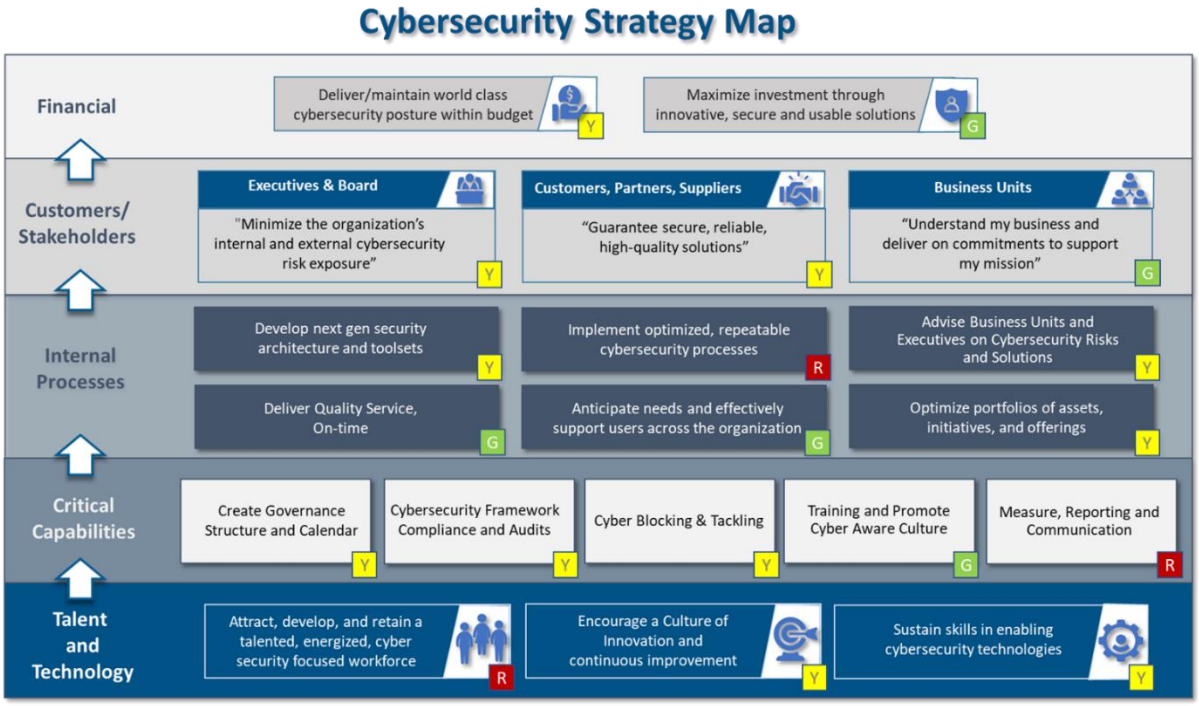
of funding and resources. Doing so ensures the development of a strategic plan that keeps the needs of the organization at the forefront.

Step Two: Develop a strategic plan that articulates the cybersecurity program's mission, vision, and objectives. Create a Strategy Map to visually demonstrate the relationship between the program's vision and its strategic objectives. This is a critical step since there is no "one size fits all" approach for building an effective cybersecurity program. The Strategy Map provides a methodology for outlining the "big picture" direction of the program factoring in organizational specifics like—goals, industry, business environment, processes and the changing threat landscape.

The program's mission and vision statements communicate the overarching direction of the cybersecurity program. In this example, the program's mission is: *"The cybersecurity program exists to protect organization assets and information."* The vision statement communicates the program's future state or destination. *"The cybersecurity program will be an enabler to the business that aligns with internal and external stakeholder requirements."* The next level categorizes the program's objectives into different categories called Perspectives. Perspectives and their order vary across industry. In the map below are examples of five perspectives that by design work together to ensure a balanced approach for an organization's cybersecurity program.

- **Financial –** To spend the optimal amount of our limited resources to protect our assets and information. What financial objectives must be accomplished? What budgetary constraints do we have to work with here?
- **Customers / Stakeholders –** To achieve the financial objectives, who are our customers and stakeholders and what needs must be met?
- **Internal Processes –** The cybersecurity program's approach to protecting assets and information requires institutionalized processes and practices and compliance with applicable legal and regulatory statutes. To satisfy this, what program capabilities are critical?
- **Critical Capabilities –** the critical capabilities outlined are a core part of a successful cybersecurity program and thus were included to illustrate their importance.
- **Talent and Technology –** To achieve these goals, how do we build a team and align individual behaviors with desired program outcomes? What technology should we implement to benefit our ongoing cybersecurity efforts?

The following is an example of a cybersecurity strategy map. It illustrates how this useful tool can be used to communicate up, down and across the organization.



Sample Cybersecurity Strategy Map

A Strategy Map offers a structured methodology for linking and prioritizing cybersecurity program capabilities to strategic business outcomes helping to ensure that the right people, processes, technology and funding are in place. The Strategy Map is an extremely useful tool as it arms the IT security leader with a one-page visual roadmap for communicating with stakeholders across functions on how the cybersecurity program will achieve its strategic vision or future state.

Scores, or status indicators, should be overlaid on the strategy map to complete the story demonstrating where the organization is in the process of achieving its target objectives and how it is improving over time. This helps the cybersecurity leaders to communicate with executives, the board, and the team so that everyone is aligned and understands the current shortcomings and when to celebrate the successes.

PRACTICE 2: Establish a Cross-functional Governance Structure for the Cybersecurity Program

Now that capabilities of the cybersecurity program are aligned with organizational goals, the next focus is how to administer or govern the program. Governance ensures that the program adheres to its mission, vision, strategic objectives, policies and practices. Governance also directs employees, customers, and partners on how to ethically and responsibly behave for ensuring the protection and privacy of organizational assets like IP and customer data.

Step One: Create a Governance Leadership Team comprised of cross-functional senior leaders. Members of this governance team are responsible for ensuring that the program operates efficiently and validates alignment with business drivers, policy enforcement, budget allocation, and program objectives, etc.

Step Two: Choose a management approach for the program. This is critical, as it provides a methodology for executing and monitoring program initiatives while also ensuring its alignment with organizational strategy and the program's mission. Cross-functional communications is an integral aspect to governance leadership. Consider using a third-party software tool to help with this. Select an application suite that provides dashboard view

Step Three: Create a governance playbook. The playbook serves as a critical repository for storing information on all respective components of the governance program like business cases, principles, policies, stakeholders, funding, oversight, and insurance policies. Information contained in this playbook represents key inputs to aspects of the cybersecurity program's strategic plan. The playbook is used and maintained by the governance leadership team. While there is a no "one-size fits all" approach for building a governance foundation, following are some components to consider including in the playbook:

- **Business case –** Statement on the organization's core business proposition helping to ensure that governance aligns with organizational goals.
- **Stakeholders –** Identifies both internal and external constituents with direct and indirect interest in the organization's cyber security program (i.e. supply chain, third parties, customers).
- **Principles –** Relates to Mission and Vision statements mapped out in the Strategy Map as well as values which will help guide individuals when making decisions for the organization.

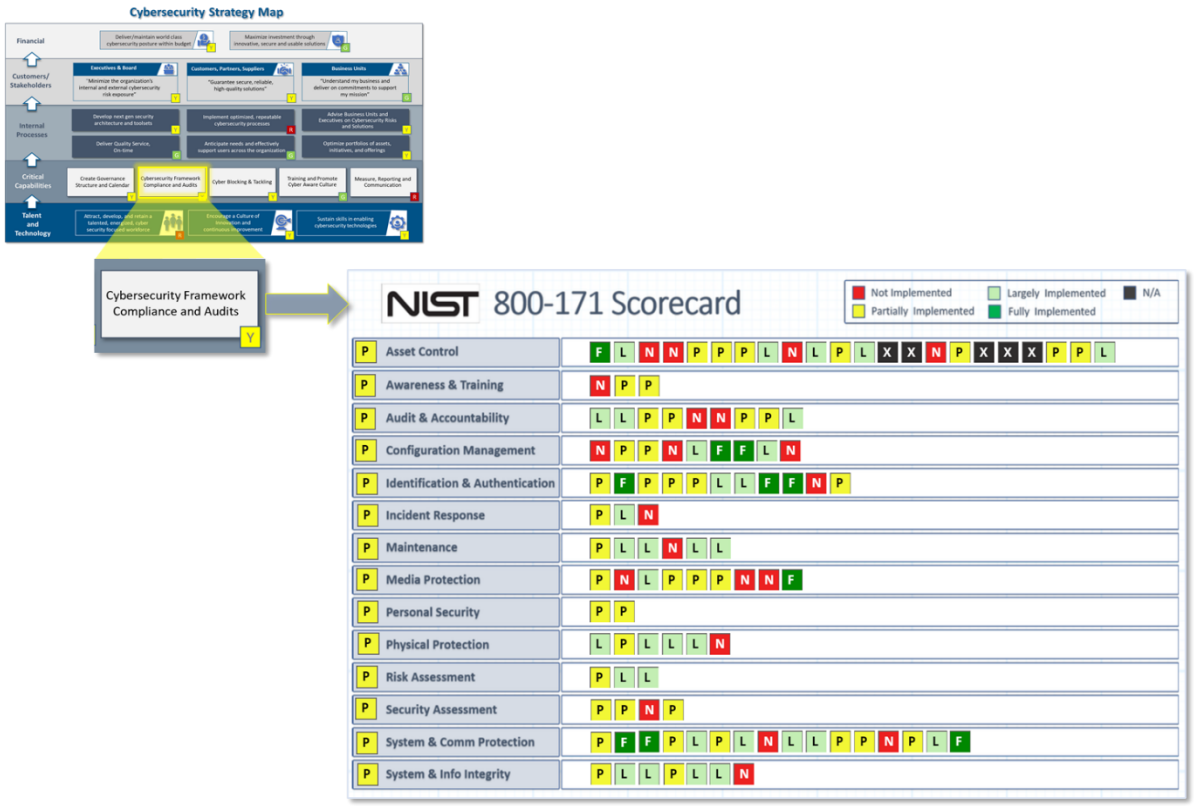
- **Ethics –** Refers to statements of ethical values that establish tone and behaviors of the program.
- **Scope of Governance –** Defines governance boundaries for who and where the cybersecurity program applies (i.e. operations, LOBs, third party partners, joint ventures).
- **Oversight –** Identifies members of the Governance Leadership Team.
- **Accountability Model –** Includes mandates of the program's security principles and policies that employees must follow.
- **Ownership Model –** Identifies accountability – who owns what. All assets and data should define owners and roles.
- **Policies –** Refers to statement of rules, practices, or actions that describe the "desired state" of the cybersecurity program.
- **Investment –** This refers to responsibility for the "goals" of the budget versus actual allocation of funding.
- **Measurement –** This refers to both effectively measuring the effectiveness of the cybersecurity program and acting on KPIs to affect improvements.
- **Set a Governance Calendar –** Ensures transparency by creating a cadence for the reporting on the "state of governance" for the cybersecurity program versus operational reporting of program initiatives
- **Enforcement –** Refers to defining consequences for violations of the governance program's principles and policies.

PRACTICE 3: Choose a Cybersecurity Framework

Cybersecurity frameworks provide structure, guidance and/or compliance requirements that include processes, practices, and technologies for organizations to use to enhance their security posture. There are dozens of frameworks for organizations to choose from, many of which include overlapping controls. In addition to cybersecurity frameworks, frameworks like the CCPA and GDPR that focus on data privacy and consumer information protection, continue to evolve.

Step One: Select a framework that best aligns with the organization's industry, management approach, and business requirements. Practices 1 and 2 recommended adopting a management approach like the Balanced Scorecard to manage the overarching cybersecurity program. This is where the organization's strategic management system and the selected framework(s) are integrated to provide a methodology for prioritizing most

important steps and tracking ongoing performance against the framework(s). For example, shown below is a sample NIST scorecard linked to the "Cybersecurity Framework and Compliance Audits" element from the Critical Capabilities perspective on the Cybersecurity Strategy Map. This integrated view shows how the Strategy Map integrates with cybersecurity frameworks for measuring and tracking ongoing compliance scores for each of the control families, and controls.



Drilldown View of the Strategy Map Integrated with the NIST 800-171 Framework

Oftentimes, the choice of which framework to adopt is effectively *chosen for the organization* as many companies and government agencies now dictate which framework requirements an organization must meet as a condition of bidding on or doing business with them. If that's not the case, consider the framework that most closely meets the organization's business requirements—and most accommodates the market served and the prospects targeted.

Listed below are some top industry cybersecurity frameworks:

1) **NIST Cybersecurity Framework** – Created by the National Institute of Standards and Technology (NIST) and developed in response to the presidential Executive Order 13636, the framework describes five functions (identify, protect, detect, respond, and recover) for managing risks to data and information security. The five functions are

subdivided into 23 Categories and 108 Subcategories. This voluntary Framework consists of standards, guidelines and best practices to manage cybersecurity risk.

2) **NIST 800-537** – This framework focuses on information security requirements designed to enable federal agencies to secure information and information systems. It also provides governmental organizations with requirements for complying with FISMA (Federal Information Security Management Act) requirements. This framework is the most granular as it contains more than 900 specific security requirements/controls to follow.

3) **NIST 800-171** – This provides a set of government regulations and requirements that must be followed by non-Federal computer systems to: (1) Store, process, or transmit Controlled Unclassified Information (CUI), and (2) Provide security protection for such systems. CUIs refer to any unclassified, but sensitive, information from the U.S. government. CUI can include anything from financial information to product patents. The regulations apply to information shared with government agencies, government contractors, and subcontractors.

4) **ISO IEC 27001/27002** – The ISO 27001 consists of international standards that *recommend* requirements for managing information security management systems. It observes a risk-based process that includes measures for detecting security threats that impact information systems. The framework includes a total of 114 controls categorized into 14 different categories for organizations to select from to mitigate security risks.

   The ISO 27002 framework includes international standards that *detail* the controls organizations should use to manage the security of information systems. The ISO 27002 is designed for use alongside the ISO 27001.

5) **FedRAMP** – The Federal Risk and Authorization Management Program (FedRAMP) is a framework designed for government agencies. The aim of this framework is to ensure that federal agencies have access to modern and reliable technologies without compromising their security. This framework provides standardized guidelines that help federal agencies evaluate cyber threats and risks to various infrastructure platforms, and cloud-based services and software solutions. It also allows reuse of existing security packages and assessments across various governmental agencies. The framework is based on the continuous monitoring of IT infrastructure and cloud products facilitating real-time cybersecurity program. A key attribute of FedRAMP is its shift in focus from “tedious, tethered, and insecure IT to more secure mobile and quick IT”.

6) **CIS v7.1** – This framework is developed and maintained by the Center for Information Security (CIS). It lists 20 actionable cybersecurity requirements for enhancing the security standards of all organizations. Most organizations view these security requirements as best practices given that the CIS has a credible reputation for developing baseline security programs. Information security controls are categorized into three Implementation Groups: Basic CIS Controls, Foundational CIS Controls, and Organizational CIS Controls.

7) **CMMC** – The Cybersecurity Maturity Model Certification created by the Department of Defense (DoD) includes cybersecurity domains, controls and processes designed to protect Controlled Unclassified Information (CUI) that resides on Defense Industrial Base (DIB) systems and networks. The CMMC mandates that any entity doing business for the DoD will be required to meet one of the five CMMC trust levels that range from "Basic Cybersecurity Hygiene" to "Advanced/Progressive". The critical factor here is that all prime contractors and their subcontractors will be required to be CMMC compliant in order to win an initial award or to renew an existing contract with the DoD. Additionally, this is not a self-attestation as an annual independent assessment of an entity's CMMC implementation must be performed by a CMMC 3rd Party Assessment Organization (C3PAO).

8) **IASME Governance** – This framework is designed for small and medium-size organizations. It provides standards for helping organizations realize adequate information protections. The IASME primarily is used to accredit and demonstrate to customers, the organization's cybersecurity readiness for protecting business and/or personal data.

9) **CCPA** – Enacted in 2018, the California Consumer Privacy Act (CCPA) refers to new consumer rights relating to: access to, deletion of, and sharing of personal information that is collected by businesses. The proposed regulations establish procedures for facilitating consumers' new rights under the CCPA providing compliance guidelines for organizations. Enforcement action under CCPA is scheduled for July 1, 2020.

10) **GDPR** – Enacted in 2018, the General Data Protection Regulation (GDPR) was developed to secure Personally Identifiable Information (PID) for European citizens. It is a global framework that protects the data of all EU citizens. The GDPR provides a set of mandatory security requirements that organizations in different parts of the world must implement if conducting business in Europe or when collecting information on any of its citizens. Non-compliance can lead to huge penalties with data breaches amounting to an organization's non-compliance.

11) **HITRUST CSF** – The Health Information Trust Alliance (HITRUST) framework addresses various measures for enhancing security. The framework was developed to address the security issues confronted by organizations within the health of organizations when managing IT security. It provides organizations with an efficient, comprehensive, and flexible guideline for managing risks, and meeting various compliance regulations like securing personal information.

The security disciplines and controls covered by these frameworks often overlap. Thus, if not already committed to one—selecting any of these will help advance the organization's security posture. The key is to adopt a reputable framework and build a comprehensive program alongside it.

Step Two: Assign an individual who is responsible for compliance with the chosen cybersecurity framework. This individual is responsible for completing the current state audit (and ongoing audits) to determine where the organization stands from a compliance perspective, and to identify current-state gaps in the cybersecurity program. This process informs of organizational weaknesses and vulnerabilities that need to be addressed for improving the organization's cybersecurity posture and moving it towards compliance.

Step Three: Determine how to close the gaps prioritizing initiatives and resources to accomplish this closure. People, processes and technology will need to be deployed to close the current-state gaps identified from step two above. Since most organizations are constrained by limited resources, a crucial process is to determine and prioritize the initiatives that need to be undertaken; resources required; and timeline for mitigation. This exercise can be challenging and typically should be based on the biggest potential risk to the organization. Below is a list of potential considerations when prioritizing initiatives and resources:

- Probability of an event occurring
- Lost productivity from outage
- Lost revenue from eCommerce system outage
- Lost revenue from customer defections (Reputation)
- Cost to regain consumer confidence (Brand)
- Cost to respond and recover
- Cost to repair and harden systems
- Liability costs (Legal and Fines)

Some additional criteria to consider for prioritizing initiatives and resources might also include:

- Time required to complete the project. Is it something that can be achieved quickly without disrupting other activities; or is it something that requires a longer timeline and more resources?
- Team and resource availability. Does the organization have the required in-house skillset; or can they readily be leveraged through current partner/vendor relationships?
- Budget. How can the gap(s) be resolved in the most cost-effective manner possible?

By no means is this list comprehensive, rather it offers insights on some factors to consider for prioritizing where and how to allocate the organization's limited resources.

Remaining Cyber Resilient - Maturing the Cybersecurity Program

To remain resilient, cybersecurity programs must adapt to changes in business drivers, risk landscapes and maturity levels. This continuous improvement requires a strategic management methodology that provides actionable steps for aligning, governing, measuring, tracking, reporting, and communicating cybersecurity program outcomes.

How can IT security leaders ensure that their organization's cybersecurity program targets the right priorities and continues to effectively safeguard critical organizational business drivers?

ESM Software works with today's IT security leaders helping them formulate effective cybersecurity strategies and evolve and mature their cyber security programs by providing them with one tool that enables them to:

- Capture organizational strengths, weaknesses, opportunities and threats all through the context of cybersecurity (SWOT).
- Create a change agenda that captures current state descriptions of core cyber capabilities and aspirational targets providing a view of where the organization needs to be.
- Develop a cybersecurity strategy map with objectives and measures to create alignment and communicate strategy and progress over time while driving transparency and results.

- Centralize cybersecurity documents, security plans, budgets and forecasts, compliance documentation, team documents, as well as ongoing reports and evidence.
- Create and track a governance calendar assigning ownership and accountability with target dates.
- Provides a framework to help prioritize strategic cybersecurity initiatives and investments.
- Track ongoing compliance with several popular frameworks including (NIST CSF, NIST 800-171, NIST Privacy, CMMC, ISO27001, etc.)

Talk to an expert today!

Sources

1. *CISO COMPASS: Navigating Cybersecurity,* Todd Fitzgerald.
2. *Building an Effective Cybersecurity Program, 2nd Edition*, Tari Schreider
3. https://www.itgovernanceusa.com/blog/how-to-conduct-an-effective-risk-assessment
4. https://www.cisecurity.org/controls/cis-controls-list/
5. https://www2.deloitte.com/content/dam/insights/us/articles/4751_2018-Deloitte-NASCIO-Cybersecurity-Study/DI_2018-Deloitte-NASCIO-Cybersecurity-Study.pdf
6. https://resources.idg.com/thank-you-2020-state-of-the-cio-summary?submissionGuid=5b6914ba-340b-4e1e-90d6-2831b161228b
7. Ponemon Institute LLC, "Separating the Truth's from the Myths in Cybersecurity" June 2018.
8. https://securityintelligence.com/articles/11-stats-on-ciso-spending-to-inform-your-2020-cybersecurity-budget/
9. https://www.iso.org/isoiec-27001-information-security.html
10. https://www.nist.gov/cyberframework
11. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
12. https://www.oag.ca.gov/privacy/ccpa
13. https://gdpr-info.eu/
14. 2020 State of Privacy and Security Awareness Report
15. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/nine-cybersecurity-metrics-every-ceo-should-track/#7f9a4129723a
16. https://www.forbes.com/sites/forbestechcouncil/2020/01/10/14-effective-tips-for-creating-and-sustaining-a-strong-cybersecurity-team/#6fc48a71a2ef