Sultanate of Oman
Information Technology Authority

Cybersecurity Governance Guidelines

Governance & Standard Division

VALIDATION & DISTRIBUTION:

	Name	Email	Issue date
Issued by	Governance & Standards Division	Standards@ita.gov.om	2017
Verified by			
Approved by	Steering Committee		

Distribution List	
1.	ITA
2.	All concerned government agencies
3.	Online publishing

DOCUMENT REVISION HISTORY:

Version	Date	Author	Remarks
1.0	2017	Governance & Standards	Creation of document

Contents

1 INTRODUCTION 3

1.1 Target Audience 3
1.2 Purpose..3

2 WHAT IS CYBERSECURITY? 4

2.1 Cybercrime and Advanced Persistent Threats (APTs)...4
2.2 Cyberwarfare...5
2.3 Other Relevant Threats 5

3 CYBERSECURITY GOVERNANCE PRINCIPLES...6

4 CYBERSECURITY TRANSFORMATION 8

4.1 Establish Current State..8
4.2 Define Target State 9
4.3 Strategic and Systemic Transformation 9

5 ESTABLISHING CYBERSECURITY GOVERNANCE 11

5.1 Step 1: Identify Stakeholder Needs...11
5.2 Step 2: Manage Cybersecurity transformation strategy. 11
5.3 Step 3: Define Cybersecurity Structure 12
5.4 Step 4: Manage Cybersecurity Risks 13
5.5 Step 5: Optimize Cybersecurity Resources..13
5.6 Step 6: Monitor Cybersecurity Effectiveness...13

1 INTRODUCTION

Cybersecurity is emerging within the fields of information security to address sharp increases in cybercrime and, in some instances, evidence of cyberwarfare. Three major factors are contributing to the need for improved cybersecurity on a global basis: ubiquitous broadband, IT-centric business and society, and social stratification of IT skills. To address cybercrime and societal changes, many governments and institutions launched cybersecurity initiatives, ranging from guidance, through standardization, to comprehensive legislation and regulation. This publication serves as initial step and provides practical guidance on the subject matter that is aligned with international good practices.

1.1 TARGET AUDIENCE

This publication is intended for several audiences who are dealing with cybersecurity directly or indirectly. These may include business managers, information security managers (ISMs), IT administrators, IT risk managers, end users, and IT auditors.

1.2 PURPOSE

The primary purpose of this publication is to enable a uniform governance, risk management and security management framework for government agencies. The secondary purpose is to provide guidance on detailed concepts and steps in transforming cybersecurity, and to align them with the existing information security strategy and processes.

This publication is primarily concerned with the type of attack that represents the highest level of danger to an enterprise and its associates. It complements the existing literature on information security and enables enterprises and individuals to harmonize their security strategies in a systemic way. The main focus is on transforming organizational security to strengthen defenses and integrate cybersecurity with the overall approach toward security governance, risk management and compliance.

2 WHAT IS CYBERSECURITY?

Cybersecurity, cybercrime and cyberwarfare as keywords have taken a prominent place in the world of security in general. This is partially due to technological evolution, and in large part to the growth in security breaches, criminal acts and the presence of information-based weapons of war.

The term "cybersecurity" in the context of information security requires an explanation because it is often misunderstood and used too broadly. For the purposes of this publication, cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches and incidents as well as the consequences. In practice, cybersecurity addresses primarily those types of attack, breach or incident that are targeted, sophisticated and difficult to detect or manage. The much larger field of opportunistic attacks and crime, usually, can be dealt with using simple but effective strategies and tools. As a result, the focus of cybersecurity is on what has become known as advanced persistent threats (APTs), cyberwarfare and their impact on enterprises and individuals.

Regardless of the common use of the term, cybersecurity should be aligned with all other aspects of information security within the enterprise. This includes governance, management and assurance. In this sense, the overall notion of security is systemic rather than linear, acknowledging the idea of being secure as a transient state that requires maintenance and continuous improvement to meet the needs and requirements by stakeholders.

2.1 CYBERCRIME AND ADVANCED PERSISTENT THREATS (APTS)

Within the universe of threats, risk scenarios and vulnerabilities, cybersecurity provides a flexible response to various types of attacks, breaches and incidents. Frequency, intensity and sophistication of attacks vary widely from what might almost be termed "harmless" to highly intricate and singular, complex attacks on a well-researched target.

APTs include attacks, breaches, infiltrations and other security-relevant events with a high to very high level of effort (or sophistication) and an approach that targets specific enterprises and/or individuals. In most cases, this involves a considerable amount of background research and intelligence gathering as well as planning and detailed preparation. Typically, an APT is delivered as a series of steps[1] designed to maximize the impact on the target. Many APTs have a professional or organized crime background. As opposed to lesser forms of attack, APT execution usually implies a significant effort in terms of time and investment. Depending on the target and its attractiveness, APTs may involve custom-made solutions that are only deployed once. In contrast to more widespread and publicly available attack vectors and tools, APTs are much less predictable, difficult to recognize and often difficult to trace back to their origins.

2.2 CYBERWARFARE

As part of the attack landscape, cyberwarfare extends the idea of APTs. Where nation states or agencies engage in attacks on critical infrastructures or organizations, the threats are augmented by the fact that the attackers may have—by definition—unlimited resources at their disposal. This includes time as a resource, given that military or government operations may take several years from the initial idea to deployment.

From a technical and managerial point of view, cyberwarfare nevertheless represents just another form of APT, notwithstanding the legal and social ramifications.
Cybersecurity should, therefore, include the possibility of direct or indirect consequences from targeted military or government activity directed against the organization, its associates or its surrounding critical infrastructure. In terms of impact, the results of open or covert warfare are fairly similar to those of criminal acts or politically motivated “hacktivism.”

2.3 OTHER RELEVANT THREATS

While cybercrime and related phenomena have seen a nonlinear increase in the past several years, other forms of threat and attack have also taken hold. These include political activism, sports hacking and targeted damage to enterprise reputation. More often than not these forms of attack are unpredictable and may not be anticipated by security managers. In this sense they are “unknown” risk scenarios and threats that must be treated as such. As a result, cybersecurity requires a strategic component that deals with the unexpected and unknown and contains elements of business continuity and IT service continuity. Consequently, the security strategies and management activities should address unknown threats and incidents, making reference to concepts of business continuity management (BCM) and IT service continuity management (ITSCM), as appropriate.

3 CYBERSECURITY GOVERNANCE PRINCIPLES

Governing, managing and maintaining cybersecurity arrangements are a challenge for business managers, security managers and auditors alike. To demonstrate the business value of cybersecurity and to balance the risk associated with attacks or breaches, the following guiding principles should be applied. While these principles are set at a high level and not exhaustive, they provide a reasonable basis for cybersecurity as an integral part of overall information security.

Principle 1. Know the potential impact of cybercrime and cyberwarfare.
The concept of cybersecurity should be seen in light of potential damage and the wide-ranging impacts of cybercrime and cyberwarfare. To adequately manage cybersecurity, the tolerable levels of risk and business impact must be known or conservatively estimated. This includes in-depth knowledge about the way in which end users may be targeted and affected by cybersecurity attacks and incidents.

Principle 2. Understand organizational and individual culture and behavior patterns.
Business value and business risk relating to cybersecurity arrangements are strongly influenced by organizational and individual culture. This is expressed by end user behavior patterns, habits and social interactions. In governing and managing cybersecurity, these factors should be taken into account and incorporated into strategic, tactical and operational security measures.

Principle 3. Clearly state the business case for cybersecurity, and the risk appetite of the enterprise.
The business case in terms of expected value and tolerable risk will determine the overall cybersecurity strategy adopted by the enterprise: the requisite effort and investment of *zero tolerance* vs. the corresponding residual risk of *living with it*. To provide adequate and appropriate security, the business case must be clearly defined and fully understood by all levels of management. This includes cost-benefit considerations as well as the prevailing organizational culture and values relative to cybersecurity.

Principle 4. Establish cybersecurity governance.
Cybersecurity exists, and is transformed, within the values and objectives of the enterprise and its members. As such, cybersecurity is subject to clear governance rules that provide a sense of direction as well as reasonable boundaries. This includes adopting and improving the organizational governance framework for cybersecurity.

Principle 5. Know the cybersecurity assurance universe and objectives.
Cybersecurity covers multiple aspects and specialized areas within overall information security. To provide assurance over cybersecurity, the assurance universe is known, defined and within the organizational sphere of interest. Assurance objectives are clear,

plausible and manageable. As many cybersecurity aspects may be outside the organizational perimeter, the associated risk and assurance issues are considered.

Principle 6. Establish and evolve systemic cybersecurity.

Cybercrime, cyberwarfare and related attacks or breaches target the weakest link in the system. As a result, cybersecurity must be understood as a system of interdependent elements and links between these elements. Optimized cybersecurity requires complete understanding of this dynamic system and the realization that security governance, management and assurance cannot be seen in isolation.

4 Cybersecurity Transformation

Cybersecurity transformation, just like any other long-term process, is based on continuous improvement and a succession through various levels of maturity. This also means that the strategy and its detailed parts will need to be reviewed and validated at regular intervals, taking into account any changes to the risk profile as well as the risk appetite defined by the enterprise.

Transformation is usually defined as a systemic shift from one stable state of the overall system to its next stable state. In between, any number of changes may happen spontaneously or in a controlled manner. In cybersecurity, transformation can be defined as progressing the overall system of governing provisions, management activities, controls and other elements from its current state to the next (target) stable state, usually by means of controlled change to certain parts, processes and other components. While this is useful as a high-level definition, some examples may help in understanding the transformation process.

4.1 Establish Current State

As a first step, the current state of cybersecurity and the existing governance model should be assessed and established. This means that, beyond the assumptions that may have existed before, cybersecurity in its present state should be described “as is,” including all weaknesses and deficiencies. Typically, this includes any systemic weaknesses previously identified (see previous section) and the pain points that have triggered the need for transformation. The underlying objective is to go from the initial observation that “we cannot go on like this” to a more constructive view of existing information security governance, management and assurance.

The current state review will also reveal any weaknesses in management attitudes. As described previously, neither the minimalist nor the “zero tolerance” attitude are likely to lead to success. Part of establishing the current state of cybersecurity is to identify the exact position of the enterprise in terms of attitudes, beliefs and security spending behavior. In summary, the governance model selected by the enterprise is likely to provide a lot of insight on what may have led to the, apparently unsatisfactory, current state.

Taking stock in this manner may be a painful exercise. However, it is indispensable as a starting point in transforming cybersecurity. Only where weaknesses have been recognized beyond doubt, and clearly articulated, will the enterprise be able to transition to an improved way of governing cybersecurity.

4.2 Define Target State

Once the existing state of cybersecurity is known and fully acknowledged, the future or target state may be defined based on weaknesses and deficiencies, risk and vulnerabilities, and the extent to which the enterprise will be able to change and adapt to the trends in attacks, breaches and incidents. Where the target state is not clearly understood, it is unlikely that a transformation approach will be successful.

Typical pitfalls include:

- Lack of realism—The target state is formulated as a wish list for perfection, rather than the next obvious (and stable) state of overall cybersecurity.
- Escalating commitment—The target state is defined as “just a little more of what we are doing now,” without incorporating the changed threat and vulnerability landscape, not to mention actual attacks and breaches.
- Blurred vision—The target state is defined based on wrong assumptions—e.g., where organizational management does not incorporate future trends in cybercrime and cyberwarfare.
- Governance model bias—The current governance model (e.g., “zero tolerance” or “we are insured”) is maintained, ignoring strong signals that it may be dysfunctional.

In transformation thinking, the target from a governance perspective is to identify the next stable—and, therefore, achievable—level at which cybersecurity will be able to meet the needs of stakeholders, and at which there will be a reasonable level of protection against attacks and breaches. Transforming cybersecurity is a repetitive and iterative exercise that resembles a life cycle rather than a one-off project.

4.3 Strategic and Systemic Transformation

The distance between the current and future states of overall cybersecurity is subject to governance as well as management. Once the target state has been identified and defined, there are two dimensions of change that need to be planned, managed and monitored. The **strategic dimension** covers setting strategy, planning and implementing high-level steps, and initiating a program and related portfolio of cybersecurity projects. The **systemic dimension** addresses dependencies between parts of the cybersecurity system that will have an impact on how change will be achieved and what will be the immediate and secondary effects.

Transforming cybersecurity in a systemic way also means that any changes will need to be examined with regard to unwelcome side effects. As an example, the deployment of an awareness program for employees may be beneficial in terms of improving vigilance and attention to detail. However, an unwelcome secondary result might be that a large number of “false positives” increases the cost of incident management and distracts attention from real (but unobtrusive) APT attacks. More complex dependencies may exist in cybersecurity systems that will only come to light if the transformation is seen as a systemic and holistic exercise.

5 Establishing Cybersecurity Governance

Information security governance in general sets the framework and boundaries for security management and related solutions. This necessarily includes formal policies, procedures and other elements of guidance that the agencies are required to follow. However, where governance in its best sense means "doing the right things," it needs to take into account that a large part of cybersecurity is concerned with handling unexpected events and incidents.

Cybersecurity governance is both preventive and corrective. It covers the preparations and precautions taken against cybercrime, cyberwarfare and other relevant forms of attack. At the same time, cybersecurity governance determines the processes and procedures needed to deal with actual incidents caused by an attack or security breach. In this context, governance principles and provisions must be reasonably flexible to allow for the fact that attacks are often unconventional, generally against the rules, and most often designed to circumvent exactly those procedures and common understandings within the organization that keep the business running.

Establish Cybersecurity governance with following six-step approach as explained below:

5.1 Step 1: Identify Stakeholder Needs

- Determine the internal and external (usually restricted) stakeholders and their interest in organizational Cybersecurity.
- Incorporate confidentiality needs and mandated secrecy in the identification process.
- Understand how cybersecurity should support overall enterprise objectives and protect stakeholder interests.
- Identify reporting requirements for communicating and reporting about cybersecurity (contents, detail).
- Clearly define and articulate instances of reliance on the work of others (for external auditors).
- Define and formally note confidentiality and secrecy requirements for external auditors.

5.2 Step 2: Manage Cybersecurity transformation strategy.

- Review legal and regulatory provisions in cybercrime and cyberwarfare
- Identify the senior management tolerance level in relation to attacks and breaches.
- Validate business needs (express and implied) with regard to attacks and breaches

- Identify and articulate any game changers or paradigm shifts in cybersecurity.
- Document systemic weaknesses in cybersecurity as regards the business and its objectives
- Identify and validate strategy for cybersecurity (“zero tolerance” vs. “living with it”)
- Identify adaptability, responsiveness and resilience of strategy in terms of cybersecurity attacks and breaches
- Identify any rigid/brittle governance elements that may inadvertently be conducive to cybercrime and cyberwarfare (e.g., instances of over control)
- Define the expectations, in alignment with strategy (“zero tolerance” vs. “living with it”), with regard to cybersecurity, including ethics and culture.
- Highlight any ethical/cultural discontinuities that exist or emerge.
- Define the target culture for cybersecurity, and develop a cybersecurity awareness program.
- Obtain management commitment for the selected strategy

5.3 Step 3: Define Cybersecurity Structure

Structure

- Define the Cybersecurity organizational structure – an appropriate platform/committee, in alignment with information security and information risk functions.
- Highlight any barriers or other organizational segregation of duties/information.
- Mandate an appropriate cybersecurity function, including incident and attack response

Roles and Responsibilities

- Determine an optimal decision-making model for cybersecurity— this may be distinct and different from “ordinary” information security
- Define high-level RACI (responsible, accountable, consulted, informed) model for cybersecurity function, including any external resources.
- Consider any extended decision rights that may be applicable in crisis/ incident handling situations.
- Determine cybersecurity obligations, responsibilities and tasks of other organizational roles (including groups and individuals).
- Ensure cybersecurity participation at the steering committee level.
- Embed cybersecurity transformation activities in the steering committee agenda.

Communications

- Establish escalation points for attacks, breaches and incidents (information security, crisis management, etc.).

- Define escalation paths for cybersecurity activities and transformational steps (e.g., new vulnerabilities and threats).
- Establish fast-track/crisis mode decision procedures with escalation to senior management.
- Identify the means and channels to communicate cybersecurity issues and information.
- Prioritize cybersecurity reporting to stakeholders by applying the principles of least privilege and need-to-know basis.
- Develop appropriate guidance for associates.

Integration

- Integrate, to the appropriate extent, the cybersecurity direction into the overall information security direction, and highlight areas of cybersecurity that are deliberately kept separate and distinct.
- Establish interfaces between the cybersecurity function and other information security roles.
- Embed cybersecurity reporting into the generic reporting methods for information security.

5.4 Step 4: Manage Cybersecurity Risks

- Determine risk appetite/tolerance levels in terms of cybercrime and cyberwarfare attacks and breaches at the board/management level.
- Align risk tolerance levels against the overall strategy (“zero tolerance” vs. “living with it”).
- Compare cybersecurity and generic information security risk tolerance levels and highlight inconsistencies.
- Integrate cybersecurity risk assessment and management within overall information security management.

5.5 Step 5: Optimize Cybersecurity Resources

- Evaluate the effectiveness of cybersecurity resources in comparison with information security and information risk needs.
- Validate cybersecurity resources in terms of specific goals and objectives.
- Ensure that cybersecurity resource management is aligned to overarching information security needs.
- Include external resource management.

5.6 Step 6: Monitor Cybersecurity Effectiveness

- Track cybersecurity outcomes and effects, particularly with a view to changes in attacks/breaches/incidents.

- Compare outcomes against transformation steps and milestones – initial (current state) and future (target state) expectations.
- Integrate cybersecurity measurements and metrics into routine compliance check mechanisms.
- Evaluate threats and vulnerabilities relevant to cybersecurity, and incorporate the changing threat landscape into cybersecurity strategy.
- Monitor the risk profile for attacks/breaches and the corresponding risk appetite to achieve optimal balance between cybersecurity risk and business opportunities.
- Measure the effectiveness of cybersecurity resources (internal and external) against defined information security needs, goals and objectives.

Conclusion:

One of the key success factors in cybersecurity governance is the adaptive and flexible nature of governance provisions. Where standard enterprise governance of IT is often supposed to set the (fairly rigid) boundaries for IT and its use, cybersecurity governance needs to acknowledge the fact that attacks, incidents and breaches always target the weakest link in the security of value chain of the enterprise. This, in turn, requires security governance design to address two dimensions:

- Basic governance provisions, e.g., expressing the intentions and overall goals of senior management
- Extended governance provisions, e.g., guidance for processes that handle cybercrime and cyberwarfare attacks or links to business continuity

The latter will often mandate a certain degree of improvisation, particularly where organizations are facing unknown risk and threats. In these cases, governance elements that are too rigid might aggravate the situation and be counterproductive. Over-control in the face of unpredictable and highly intelligent attacks and breaches should be avoided and actively remediated.