



* Akshay Garkel

Institutionalizing Cyber Security Strategy



"It's time for businesses to realize that they need to prepare and respond to cyber threats with a proactive & offensive strategy for today and the times to come."

Cyber Security Strategy: Developing a robust strategy and framework, to remain resilient in the dynamic threat landscape

Contents:

- Current Security Threat Landscape
- Establishing of Cyber Security Strategy
- Sustenance & Compliance
- Management Commitment
- Cyber Security Framework
- Conclusion




Current Cyber Security Threat Landscape:

The days when risks were easily understood and predictably managed are over. Cyber attackers, who once acted in isolation, have evolved into organized, skillful, extremely agile profit-driven businesses that usually operate internationally to make it harder for national crime agencies to track them down.

Experts estimate that cyber crime costs the global economy as much as \$600 billion annually underscoring the massive growth in malicious activity online and rapid expansion of the ecosystem of internet-connected devices, commonly known as the "Internet of Things".

The massive growth is largely attributed to the proliferation of new technologies, as well as the financial sophistication of top-notch criminal hackers and cyber crime-as-a-service.

Some companies fall victim to criminal organisations that are trying to launder stolen funds, while other attackers are simply on a 'fishing' expedition to see if anything of value or interest is out there. Consider the following examples of data security breaches in recent times,

-  Yahoo: Data stolen of all 3Bn accounts
-  Uber: Data of 57Mn customers was stolen by hackers
-  Facebook: Data privacy scandal embroiling Facebook, which may have revealed that up to 87 million users data

Whatever the motive, cyber crime is expected to grow, both in number and the level of sophistication, as the push towards globalization & digitization, integration of technology systems converges to increase the risk of attacks.

The best way for organizations to protect themselves is to be proactive rather than reactive.

Organizations should analysis their cyber security health status and conduct a cyber security risk assessment to develop a robust "Cyber Security Strategy". It will complement their business dynamics and protect them from new arising threats.



Establishing Cyber Security Strategy:

Security strategy in any organization starts with an in-depth analysis of their business. It can be used to effectively articulate core security objectives, aligning them with business goals.

It is an important process which details series of steps necessary for an organization to identify, remediate and manage risks while staying compliant.

An effective security strategy should be comprehensive and dynamic, with the elasticity to respond to any type of security threat.

Following tactics to be considered while developing cyber security strategy,



1. Risk Assessment
Analyzing risk helps you determine your tolerance levels for risk and which you can accept, avoid, transfer, or prevent. Risk analysis can help determine how to best budget and prioritize security initiatives.



2. Standards & Frameworks
Ensure that your security model is developed based on Security standards, COBIT, COSO, NIST guidelines and frameworks.



3. Business Impact Analysis
Identification of critical business process & assets and threats associated with it.



4. New wave technologies & risk arising from them
Organization planning to adopt IOT, Blockchain, Artificial Intelligence (AI), Business Analytics (BA) and Machine Learning (ML) needs to ensure that these technologies compliment their business and will return greater ROI.



5. People
Ensure that resources are deployed with relevant skill set.



6. Process
Based on industry best practices ensure the processes are designed, implemented and monitored to ensure it effectiveness.



7. Regulatory & Legal Requirements
Ensure that your strategy is developed in line with requirements, guidelines, and circulars and notifications laid out by the regulatory body.



8. IT Security Awareness Program
Awareness programs should be established to ensure that all employees, contractors, third-party, vendors, agents and customers are aware about organization's information security policies, their roles & responsibilities, threats, vulnerabilities and risks.



9. Vision & Mission
Cyber Security Strategy should be developed considering organization vision and mission to ensure the strategy developed is effective and benefits the complete ecosystem.



10. Lesson Learnt
Ensure the finding are considered from lesson learnt and incidents occurred in past to best budget and prioritize security initiatives.

Strategy Priority Matrix: -

High

Investment	<ul style="list-style-type: none"> • 5. People 	<ul style="list-style-type: none"> • 4. New Technology Adoption • 1. Risk Assessment • Threat Intelligence, Bug Bounty
	<ul style="list-style-type: none"> • 2. Standard & Framework • 6. People • 8. Security Awareness Program • 9. Vision & Mission • 10. Lesson Learnt 	<ul style="list-style-type: none"> • 3. Business Impact Analysis • 7. Regulatory & Legal Requirements

Low Complexity → High

Indicative would vary across environments

Sustenance & Compliance - Ensure that security strategy is reviewed on an ongoing basis. The established security framework should be audited on a periodic basis to ensure effectiveness and compliance in the continual improvement journey



Management Commitment –

Align your security strategy with business objectives to ensure management approval.

Management approval and executive sponsorship is the most important factor in the success of a security program.

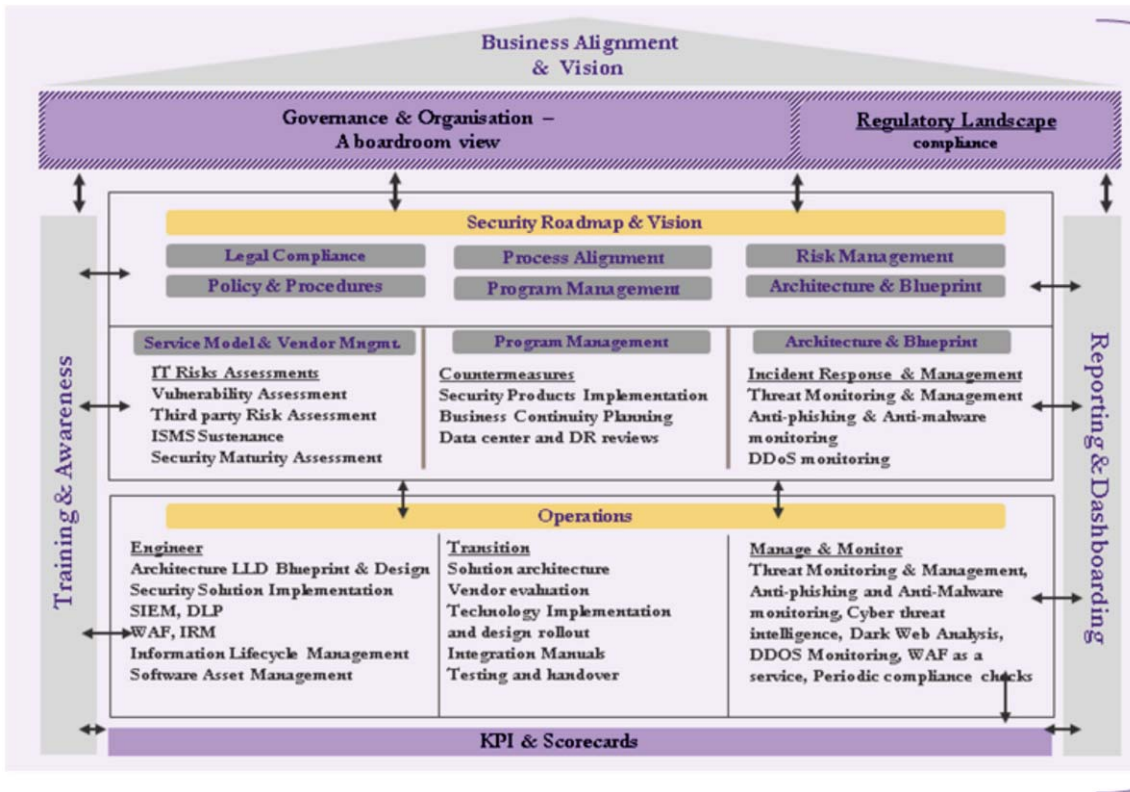
This can lead to improved employee adherence to policies and increased security budgets leading to implementation of effective solutions that support the strategy

It is imperative for security strategists to have everyone required on board, so that they know the value of the assets being protected and the real cost of breaches which can then help determine current and future security requirements.

Each strategic objective need to adhere to the following tenants, goals, and objectives:

- Acquisition and implementation of common enterprise security tools to maximize cost reductions with economies of scale. Technologies, tools and solutions must be integrated to the maximum possible capacity providing automated enterprise-wide visibility into the security structure of the organization's information and information systems.
- Consideration should be given to leveraging and integrating existing investments to the greatest extent possible to conserve constrained budgetary resources.
- Solutions should not be conceived in a fashion where consideration is given towards addressing only a single risk or requirement. Solutions should collectively be able to mitigate risks while addressing cost efficiency.

Cyber Security Framework:



A framework driven approach adheres to adequate and holistic coverage of your Cybersecurity posture and helps align your processes to best practices.

Conclusion

Strategic implementation, testing and review activities should be planned as part of the development. Ideally, the executive committee and the Board need to review the cyber security strategy with the CISO and understand the implications and provide feedback on each strategic objective. The final approved and signed off cyber security strategy document should be communicated to the intended audience. To measure success of the security strategy, one must ensure that initiatives provide enough flexibility to adjust to abrupt changes in business, legal and technical environments.

The strategic task must generate a sense of eagerness among the personnel, so that they follow the plan and take personal ownership ensuring its success.

A cyber security strategy is not a one-time activity and thus assessments must be done periodically to measure effectiveness of implemented initiatives. It should be revised as and when there are changes in legislation, business and technology landscape.

** Akshay Garkel, Partner, Grant Thornton India LLP. Akshay comes with an experience of 18+ years in IT Risk Advisory and Cybersecurity.*

Subscribe
today



Want new issues of **Directors & Boardroom** magazine delivered to your email every month ?

write to us at
info@iodglobal.com