

Analysing Security Investments

Cybersecurity for Business Leaders

Version: 1.0
Document Ref: ReBIT/2018/CBI/RI-103

Cybersecurity Business Insights

Never invest in a business you cannot understand.

- Warren Buffett

Abstract:

There are expectations from board members, CEOs and senior executives at banks to implement robust cybersecurity practices. Cybersecurity no longer is a security risk limited to IT functions of an organization and there is an increasing recognition that it is now an integral part of operational risk management. This paper describes how security gets implemented through controls and what business leaders need to know about it.

Authors/Contributors

Vivek Srivastav	SrVP, Research and Innovation, ReBIT
-----------------	--------------------------------------

Disclaimer: *The mechanisms suggested in the document represent the view of the author and are indicative. There may be alternative ways to achieve the same objectives. Organizations may consult experts and implement a strategy most suited and aligned with their own organizational objectives.*

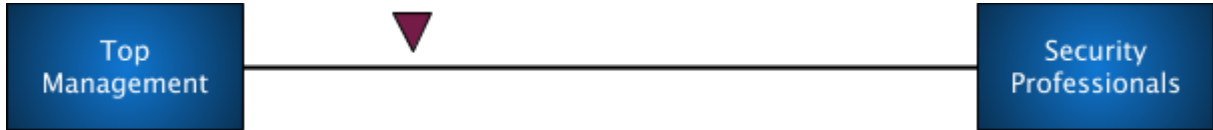


© ReBIT, All Rights Reserved

Revision History

Version	Date	Comments
1.0	13 Oct 2018	Initial Draft

Document Spectrum



Acknowledgements

Contribution to the content through discussions and review was provided by Mr. Jayaraman Pazhamalai, SVP System Audit at ReBIT and Mr. Nandkumar Saravade, CEO ReBIT

Table of Content

1. Overview	3
2. CIA Triad	4
3. Layered Approach to Security	5
3.1. The People, Process and Technology	5
3.2. Transmission of Control Effectiveness	6
3.2.1. Product Security	7
3.2.2. Configuration	8
3.2.3. Controls	8
3.2.4. Monitoring	10
3.2.5. Audit	11
3.2.6. Regulation	11
4. Cyber Risk Analysis	11
5. Summary	12

1. Overview

A framework and a concept of how to implement security is presented in this paper. In the *Cybersecurity Business Insights* paper on *Key Baseline Security*¹ we have suggested some controls that are essential for organizations to implement. Qualitative reasons for why the suggested key baseline controls are essential were only briefly presented.

When considering investment in security, a potential conflict arises between cost centers and profit centers. Security controls and investment are a cost center. In contrast, business goal is to generate revenue and is a profit center. Costs generated by the IT and security department eat up profits generated by the business side. Additionally, many of the security controls introduce friction and reduce usability of systems in the interest of security. Consequently, the business side sometimes views the IT department as spending money, reducing profits, and making it more difficult for the business to generate profits. Nevertheless security is important and a necessary investment as cost of failures are high.

Security is about risk management. There must be some basis for prioritizing investment in cybersecurity controls. When it comes to cybersecurity there are plethora of controls available and a large number of security products. How do we know what products we should invest in? The organization's budget is limited and business drivers and risk appetite should drive and dictate investment in security. Given this, mature organizations must use a methodical risk analysis framework and cost-benefit models to make investment decisions in cybersecurity products and control implementation. While risk management can provide security investment decisions, better security posture, implementation of security controls and maturity in adoption of best practices, it can also provide trust and confidence to partners and positively impact business profits. There are some general principles that should be considered for strengthening cyber security in an organization:

- **Security by design:** The cost of security incident increases progressively in the development phases², with costs being significantly higher when security has to be applied retroactively after the product is deployed.
- Take risk-informed **decision** investing in security controls: The investment in security should be a business decision based on risk analysis, the organization's appetite for taking risks and accepting them. The cost of control must not exceed cost of asset.
- **Implement baseline security first:** some controls are essential to implement because several other controls depend upon these baseline controls to be available. In these cases, these baseline controls are necessary to implement.
- Investment in control should **consider operational cost for effective implementation:** Many controls require effective implementation which

¹ ReBIT, *Key Baseline Security*, Oct 2018, Cybersecurity Business Insights

² *What Does It Cost You To Fix A Defect? And Why Should You Care?*, Oct 2000, <https://www.jrothman.com/articles/2000/10/what-does-it-cost-you-to-fix-a-defect-and-why-should-you-care/>

requires resource investment, if these costs are not factored and the resources not effectively deployed then the benefits are lost.

- **Commitment from the top:** The security creates friction and might affect usability, it requires additional investment and could delay product deployment. To overcome such challenges and address these concerns, a culture of security and commitment requires top management support.

A brief outline of the risk analysis framework and corresponding concepts are presented in this paper. We will separately deal with these topics in more detail in a separate paper on “Cybersecurity Tools for Business Leaders.”

2. CIA Triad

The primary goal and objective of cyber security management is to provide confidentiality, integrity and availability (also known as CIA triad). The implementation of security controls is evaluated on how well they address these three core information security elements. A security solution should adequately address each of these elements. The vulnerabilities and threats are also measured in terms of how they impact these three core elements. Consequently, these three principles are considered the most important elements within the realm of security implementation.

Confidentiality	<p>The measure used to ensure the protection of secrecy of data, objects or resources. The goal of confidentiality is to prevent or minimize unauthorized access to data. If a threat exists against confidentiality, unauthorized disclosures may take place. The data needs to be protected in storage, during processing and in transit.</p> <p>A breach of confidentiality is not necessarily limited to directed attacks, but it can happen because of human error, oversight, ineptitude, poor software design or software bugs.</p>
Integrity	<p>Integrity relates to protecting the reliability and correctness of data. For integrity the objects must retain their veracity and modification should only be allowed through authorized means. Alterations should not happen while the object is in transit, storage or in the process.</p> <p>Integrity violations can happen because of intentional manipulation, human error, oversight, ineptitude of errors in commands, codes or scripts. The malwares and viruses try to violate the integrity of the system.</p>
Availability	<p>Availability means that authorized users are granted timely and uninterrupted access to objects. The objective is to ensure authorized access at an acceptable level of performance, ability to quickly handle interruptions, maintaining redundancy in the system, maintaining system backups, having a disaster recovery (DR) and business continuity plan (BCP).</p>

3. Layered Approach to Security

The organizational assets need to be protected and the security controls we put in place need to ensure that confidentiality, integrity and availability are maintained in accordance with organizational policy and tolerance levels. Because of these different dimensions of security elements, often multiple controls are required to protect organizational assets. Implementing multiple controls helps reduce cyber risks. This concept of implementing multiple security controls to secure organizational assets is known as "layered approach to security" or "defense in depth". The goal of implementing multiple security controls is to ensure that the "residual risks" are within the tolerance level for the organization.

We will look at how to quantify residual risk through risk analysis exercises but first let's look at some additional concepts about types of controls and where they are implemented.

3.1. The People, Process and Technology

Security are always implemented through controls. All controls have people, processes or technology aspects in them. When a security technology is implemented, then there are certain processes to follow for utilizing the technology effectively and people should have an understanding of how to use the technology. Consequently, in cybersecurity, the community always talks about this people-process-technology triad. This triad and their relationship is shown in the diagram below:

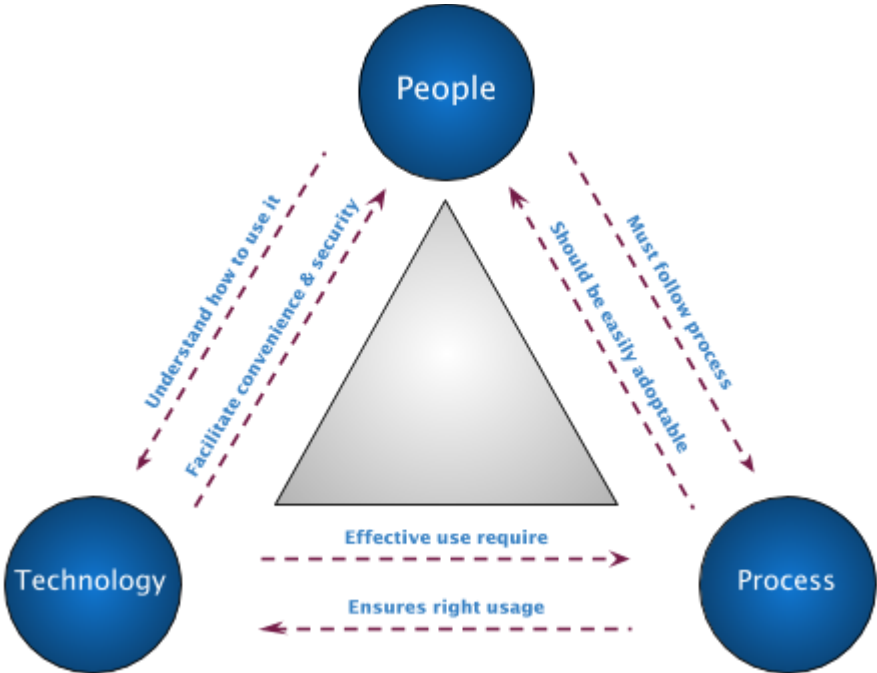


Fig-1: The People, Process and Technology Triad

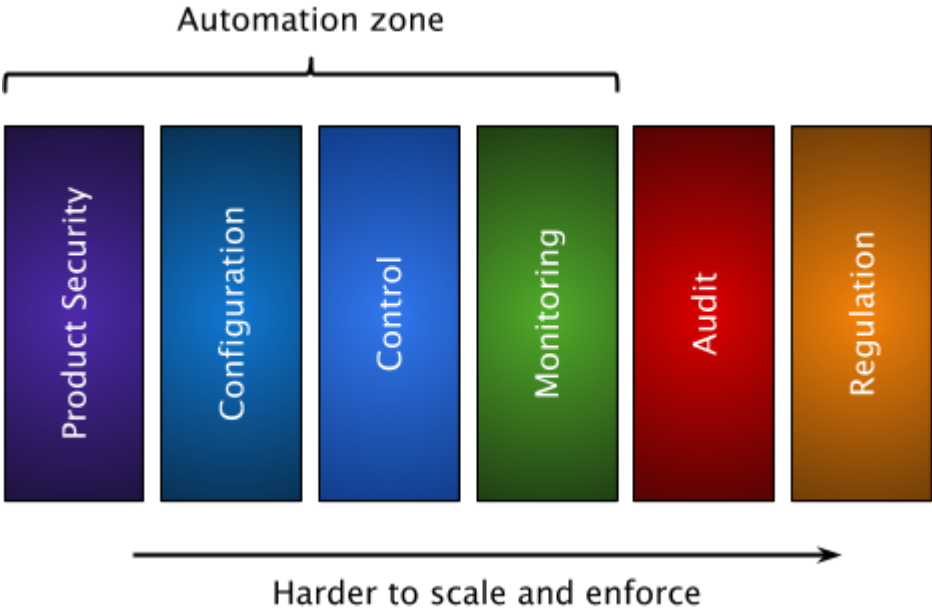
One of the things to realize from this diagram is why customer awareness is such an integral part of cybersecurity and why right governance and process are important to

follow. Security is not just about technology. This relationship also governs investment required in technology. For example, if an organization has very mature security awareness in its employee who follow defined process and can distinguish good and bad behavior, then the organization might decide to spend less on the technology and rely on mature behavior of its employees.

Another, aspect to realize is that, in some cases, technology solutions might not be available or may be prohibitively expensive. For example, if data is shared with a third party, how that data is used is outside the scope of any enforceable technology solution. Then, in such cases, an organization has to rely on contractual agreement and perhaps audit to ensure that contractual agreement is being followed. This kind of limitation and a need to rationalize how security controls work gives rise to the notion of “transmission of control effectiveness”.

3.2. Transmission of Control Effectiveness

The security could be implemented at various different levels.



At one end of the spectrum is the technology used to implement the business solution, which is where the security risks should be mitigated and on the other end is the regulation which sets the expectations for safe operation of the IT infrastructure by the banks. We would expect that a system built with strong security focus, configured appropriately and operating with the right network controls would have high cyber resiliency. Despite this we find that there are large numbers of cyber incidents and security breaches.

Why are we not able to get this right?

One of the reasons is that there is a lack of understanding of how to invest in security and consequently a commitment to strengthening the controls in the technology. While there has been a lot of focus on security and the second tier (see the “Three Line of

Defense” Cybersecurity Business Insight paper), security in design, accountability and ownership about security is something that is at the core of the problem. An organization, when it adopts a culture of security becomes more resilient to cyber crimes. Developing a culture of security transcends through stages of training, awareness, mindfulness and security first culture. While the human element is perhaps the most important aspect of security the controls implementation happens at multiple tiers which are discussed in the following sections.

3.2.1. Product Security

Secure by design is an important principle to focus when an organization is looking at solving a business problem using technology. If a security problem can be solved within the technology tier, it should be solved there. The Secure Software Development Life Cycle (S-SDLC) process is focused on mitigating security risks at the software level. If these risks are mitigated within the software, then security risk in the subsequent layers will pose lower risks. If there is a need for data security and confidentiality, then the technology can provide solution in form of encryption of data at rest and in motion, concepts such as electronic consent may be utilized to enhance security and enforceability through the use of technology.

Software solutions are usually not designed with security in mind. Until recently, there was no focus on integrating “security” into the software development life cycle. Over the last several years, the secure software development life cycle-SDLC) process has gained momentum and larger organizations have started to incorporate S-SDLC into their product design. Adding “security” in the software development lifecycle increases cost and time, but it is worth it. Many larger organizations set up PSIRT (Product Security Incident Response Team) to track vulnerabilities in their products and notify their customers about patches and fixes as they are discovered. When purchasing software products from a vendor, the organizations must ensure that the vendor has a PSIRT team and mechanisms to report vulnerability and takes accountability for the software vulnerability for the life of the product. When developing software or getting it developed from a vendor, the security requirements must be baked right from the start of product development. The S-SDLC process provides a good framework for this.

In an industry largely driven by outsourcing and custom products, where the cost of development is an important element, the timed delivery pressures are there, the invisible hands of vulnerabilities and software weaknesses are stronger and creeps into the product over period of time. Any software once deployed takes a life of its own and requires continuous enhancements and security review, patching and upgrades. These days, the softwares are incredibly complex pieces and often built using large number of reusable components. Vulnerabilities might be discovered in any of these dependencies or it may be found on the application servers or the operating system on which the software is deployed. Any of these vulnerabilities may be exploited. For e.g., in case of Equifax data breach, the vulnerability in the “struts library” was exploited³. Majority of the web application developed in Java programming language uses “struts”.

³ Equifax, Apache Struts, and CVE-2017-5638 vulnerability, 15 Sept 2017
<https://www.synopsys.com/blogs/software-security/equifax-apache-struts-cve-2017-5638-vulnerability/>

This complexity is not well understood by the organizations and business owners and we generally look at the software delivery as a fixed timeline project, consequently as the vulnerability gets discovered in the software and fissures appear in the security of the applications we become increasingly vulnerable to exploits.

The security is not a problem of the CISO or the second line of defence⁴, it is the problem of the business owner and this recognition is what would help us ensure that we have secure products and right controls to be cyber resilient. Consequently, the business owner must ensure that security requirements are captured into the product design and selection.

3.2.2. Configuration

The second tier is the configuration tier. Any software solution or a product security solution needs to be configured appropriately for a safe operation. In the Nirav Modi case, the misuse of SWIFT to send unstructured MTx99 SWIFT messages is a problem of inappropriate configuration. The SWIFT systems could have been configured to allow operators to use only specific message types. A software or a technology solution is designed with flexibility in mind so manageability, features availability, customizations are possible. This configurability also adds to complexity and consequently there is a need to harden the technology solutions through proper configuration.

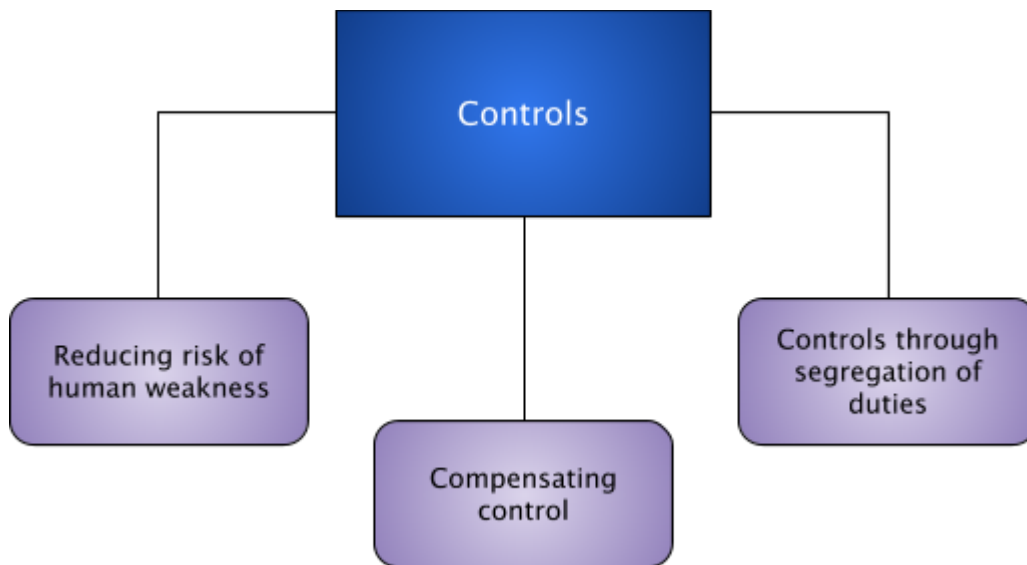
- Ensure that proper access control and authorization is implemented
- Ensure that the system is configured so it can only be used for the intended purpose
- Implement change control mechanism so all configuration changes are tracked

Appropriate configuration would require domain knowledge and application expertise and would have to be maintained and managed.

3.2.3. Controls

Third tier important for security implementation is the “Control” tier. Many security and frauds measures require instituting processes that focuses on human element to ensure safe operating environment. Any technology solution requires understanding of configuring and utilizing a solution effectively. This comes from user training, cybersecurity awareness and a culture of security. Sometimes, the security is not just a technology problem, for e.g. a proper segregation of duties, maker-checker mechanisms is essential to create a safe functional business environment that provides high assurance. Sometimes a technology or a business process might not be able to provide the desired security assurance, in such cases compensating controls would be required. For example, many ATM continue to use Windows XP, given that Microsoft has stopped supporting the operating system, the organizations using ATMs must implement and focus on several compensating controls such as applications whitelisting, limit connectivity to only authorized network resources and enabling firewalls.

⁴ ReBIT, Three Line of Defense, Oct 2018, Cybersecurity Business Insights



Consequently, the control measures are important part of the cybersecurity triad in ensuring a robust cyber resilient environment within an organization. What can't be solved in technology and configuration has to be addressed through "control".

Cybersecurity Term: Exposure

When vulnerabilities are discovered in software solutions a patch or fix might not immediately be available or deployable (the business owner might want to ensure that there is no disruptions when the patch is deployed and might need to perform some testing before the patch is rolled out).

While these vulnerabilities are not fixed/patched, the organizations run the risk of these vulnerability being exploited. The time, between when the vulnerabilities becomes known to the time that they get fixed/patched, is called exposure. Average time it takes organizations to patch these vulnerabilities is quite high. As per EdgeScan vulnerability report, 2018 it takes up to 67 days to patch the vulnerabilities. The financial sector takes an average of 176 days to patch vulnerabilities⁵.

TIME-2-FIX (WEB APPLICATIONS / LAYER 7)

7 Days 22%	8 - 30 Days 21%	31 - 90 Days 30%	90+ Days 25%
---------------	--------------------	---------------------	-----------------

Average time to close a discovered vulnerability is 67 Days

Source: Edgescan⁶

⁵ Financial sector takes up to 176 days to patch security flaws, 2 June 2015, <https://www.zdnet.com/article/financial-sector-takes-176-days-on-average-to-patch-security-vulnerabilities/>

⁶ EdgeScan, Vulnerability Statistics Report, 2018, <https://www.edgescan.com/wp-content/uploads/2018/05/edgescan-stats-report-2018.pdf>

A robust security team in organization must focus on reducing this exposure time through a proper patch management process.

During the time that the software solution has an exposure, security team might need to put compensating controls to ensure operations without compromising the security.

There are mainly three types of controls:

- Physical Controls (such as walls, doors)
- Administrative Controls (such as policies, different type of checklists, company procedures/processes)
- Technical Controls (such as firewalls, anti-virus, IP whitelisting)

Each of these categories has six different approaches that could be considered:

Deterrent	Preventive	Corrective	Recovery	Detective	Compensating
Intended to discourage a potential attacker	Intended to avoid an incident from happening	Fixes components or systems after an incident has happened	Intended to bring the environment back to normal operation	Helps identify an incident activity and intruder	Control that provides an alternative measure of control

Controls should be designed to balance all the areas namely preventive/detective & corrective. Controls that mitigates significant risk exposure (combination of threats and vulnerabilities) may benefit from automation.

3.2.4. Monitoring

In an imperfect world with human weakness, complex dependencies and cyber crime, a continuous process of monitoring the security status of the organization is required. On one hand, it is important to fix the vulnerabilities as they become known and gets exploited, on the other it may be strategic decision an organization may take to themselves deploy resources to discover vulnerability. The fourth tier “Monitoring” is an important mechanism that needs to be instituted in the second line of defense to plug vulnerability issues that gets discovered in products and their dependencies over period of time. There are multiple strategies for monitoring that the security teams must consider:

- **Security gates at the production:** Organizations must institute a process to perform vulnerability assessment and penetration testing (VAPT) of a solution before they are rolled out to production. This will ensure that risks are understood and right compensating controls are implemented to guard against any identified vulnerability.
- **Continuous vulnerability assessments and scans:** Once the solution has been deployed, there should be continuous monitoring and checks against vulnerability databases, vulnerabilities and patches shared by the vendors and a robust patch management process must be setup.

- Advanced monitoring techniques such as **Red-Teaming** might be utilized by larger organization and use internal resources to discover vulnerabilities in the software solutions before they are discovered by cyber criminals.
- **Responsible Vulnerability and Bug Bounty Programs** are other mechanisms which can help organizations discover vulnerabilities through engagement of external security resources.

Automation

The first 4 tiers, there is scope of automation.

- In the technology tier, the S-SCLC process might benefit from CI/CD (continuous integration and continuous delivery) mechanisms
- The configuration tier can benefit from CMDB (configuration management databases) to ensure that right configurations are deployed and there is a proper change control mechanism in place.
- The control tier can benefit from workflow driven process automation
- Continuous vulnerability scans and automated patching may be implemented in the monitoring tier.

3.2.5. Audit

The audit, which is the fifth tier in the security implementation layers, ensures that right configuration, governance and processes are being followed. They are the independent eyes of the board and senior management and ensures that security objectives are met with the controls that are implemented. The audit ensures that the first line of defense and the second line of defense are operating effectively. An internal IT security audit process must be instituted on a periodic bases.

3.2.6. Regulation

The regulation looks at the systemic risk and need for ensuring the consumer trust in the financial stability of the economy and the mitigation of the cyber risks. It is imperative that financial institutions are operating a sound and secure systems to prevent large scale disruptions to the economic engine. While the regulation should be principle based it should not become an exercise in compliance. If organization take a compliance led approach to security implementation, the gaps in cybersecurity will not get addressed, because it is not possible to be comprehensive and describe in detail all that is needed to ensure cyber security of the sector.

4. Cyber Risk Analysis

There are two types of analysis that can be performed to understand the cyber risk a business is exposed to:

- **Quantitative risk analysis** is a scientific approach to quantify the business impact of cyber threats or vulnerabilities on critical and sensitive assets of the organization. The quantification depends upon the value of the assets, expected

loss to either the asset value or the business in case of a cyber incident and probability of such occurrence. Such loss is compared against the cost of security controls and the amount by which they reduce the expected loss. This quantification in monetary terms helps the organization do a cost vs benefit analysis and make an informed decision on security investment in specific controls.

- **Qualitative risk analysis** assigns subjective and intangible values to the loss of an asset. Qualitative risk analysis is based on evaluation of possible scenario that creates risk. Rather than assigning exact monetary value to possible losses, the threats are ranked on a scale to evaluate their risks, costs, and effects. T-shirt size estimates or low-medium-high classification may be used. The process of performing qualitative risk analysis involves judgment, intuition, and experience. The qualitative risk analysis may use techniques such as brainstorming, Delphi technique, storyboarding, questionnaires, interviews with domain experts etc.

A combination of quantitative and qualitative risk analysis should be used to then make informed decision to selectively invest in strengthening controls.

5. Summary

The primary goal of security is enshrined in the CIA triad, I.e maintaining the confidentiality, integrity and availability of organizational assets and services.

Criminal exploit weaknesses in human nature first to gain access and then the weaknesses in the software or the process to cause damage. We make an argument that it is increasingly difficult to enforce and scale security as we move from left to right on the tiers for implementing security. Even if we build high castle walls and deep moats of security products around the organizations, but lack a process to address the security vulnerability continuously we will not get security right.


Security is implemented in layers and implementing security in one tier does not necessarily mitigates risks that emanates in other tiers. Consequently the security need to be effectively implemented at various tiers. In each of these tiers, it is important to consider the people-process-technology triad of cybersecurity.

The investment in security should be based on informed decision making. This comes from a combination of qualitative and quantitative risk analysis and prioritization based on them.

This article has provided some context on how to look at implementing security within an organization. We briefly have touched upon the cyber security risk analysis and it could be used to make scientific and informed decisions about security investment. In a subsequent paper on “Cybersecurity tools for the Business Leaders”, we will discuss the tools available for the board and senior management for cybersecurity analysis and assessment.

Stay Connected

Reserve Bank Information Technology Pvt. Ltd
<https://rebit.org.in>

 **LinkedIn**
<https://www.linkedin.com/company/reserve-bank-information-technology-pvt-ltd>

 **Twitter**
<https://twitter.com/reservebankit>

 **Email**
communications@rebit.org.in

Cybersecurity Business Insights Paper Series

Cybersecurity is an operational necessity, and board members and senior executives are required to adequately address the risk emanating from cyber crimes and data breaches. The “Cybersecurity Business Insights” paper series is designed to provide coverage of cybersecurity topics most pertinent to business leaders. These topics will enable senior executives in setting the right governance structures and policies, creating the right expectations and defining priorities, building a talent pool to address the cybersecurity needs of the organization and take a risk-driven informed approach to cybersecurity implementation within their organizations.

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. ReBIT disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any act or omissions made based on such information. ReBIT does not provide legal, regulatory, audit or tax advice. Readers are responsible for obtaining such advice from their own legal counsel and other licensed professionals. No part of this publication may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the author.

About ReBIT

Reserve Bank Information Technology Private Limited (ReBIT), has been set up by the Reserve Bank of India to serve its IT and cybersecurity needs and to improve the cyber resilience of the Indian banking industry.

Copyright © 2016 ReBIT All rights reserved

ReBIT and its logo are registered trademarks.

No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Subscribe to ReBIT’s Cyber Pulse Monthly Newsletter

<https://rebit.org.in/newsletter>

