

U7D3B3sh>5l>>o



ShadowPlex™

Reserve Bank of India (RBI)

CyberSecurity Mandate Compliance

Jan 2018



Table of Contents

1. Introduction	2
2. Framework Overview.....	2
3. RBI Cybersecurity Framework’s Requirements and Acalvio.....	3
3.1. Annex – 1: Baseline Cyber Security and Resilience Requirements.....	6
3.2. Annex – 2: Setting up and Operationalising Cyber Security Operation Centre (C-SOC)	9
3.3. Annex – 3: Template for Reporting Cyber Security Incidents	11
4. Summary	12

1. Introduction

The ever-increasing threat landscape and seemingly never-ending list of breaches discovered each year have driven tighter security controls by many enterprises globally. In addition, compliance requirements are not meeting the sophistication of today's attacks, nor are prepared for tomorrow's attacks. In response to this gap, many large corporations are implementing additional controls above and beyond compliance requirements to ensure they are on the forefront of defending against these sophisticated adversaries. One such example of defining additional security controls is the Reserve Bank of India (RBI)'s Cyber Security Framework in Banks. This framework defines requirements that today's modern financial organization should adopt to protect themselves from the evolving attack techniques developed by cyber attackers every day.

"Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond/recover/contain the fall out."

Cyber Security Framework in Banks, RBI, 2016

2. Framework Overview

The "Cyber Security Framework in Banks" consists of a general circular, supported by three annexes. The core concepts defined in the circular make it clear that the RBI felt that while banks are implementing a basic level of IT security controls to prevent compromise, they were not doing enough to reliably detect, respond to, and contain threats that have penetrated their defenses. Among the elements in the guidelines, the following stand out in support of this goal:

- **Arrangement for continuous surveillance** – This guideline mandates the creation of a Security Operations Centre (SOC) to ensure "continuous surveillance". Annex 2, which details the SOC requirement, highlights the surveillance requirement: "The Cyber SoC has to take into account proactive monitoring and management capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytics". It is important to note that the SOC guidelines specifically call out the use of honeypot services. This is one of the very few specifications of a particular technology by the RBI framework, which speaks to the clear value of honeypot solutions in detecting and responding to advanced threats.
- **Cyber Crisis Management Plan (CCMP)** – Banks must immediately begin work on their CCMP, which should address incident Detection, Response, Recovery and Containment. Such a plan is completely focused on post-incident activities, acknowledging the need for banks to re-focus on threat prevention.
- **Incident Notification** – Banks must promptly notify the RBI of all "unusual" cyber-security incidents whether successful or not. The incident template form (Annex 3) requests notification within two to six hours. The notification template in Annex 3 includes elements related to the details of the attacker's identity and methods. This places a huge burden on the

banks. They need effective, broad threat detection and analysis tools to be able to properly characterize the attack in such a short timeframe. The traditional log collection and analysis approach clearly will not work – it might take days just to get the logs together to start the analysis.

“The systems that NEED to be put in place as a part of the Cyber SoC requires the following aspects to be addressed....Counter response and Honeypot services”

Cyber Security Framework in Banks, RBI, 2016

3. RBI Cybersecurity Framework’s Requirements and Acalvio

RBI Framework Requirement Reference	Acalvio Support
Baseline (Annex 1)	
Key Points Preamble: b. It is important to endeavour to stay ahead of the adversary. c. Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time. d. It is important to keep the vigil and to constantly remain alert.	Acalvio provides broad, real-time vigilance of adversaries at all stages of the cyber kill chain.
Item 2 – “it is essential to enhance the resilience of the banking system by improving the current defences in addressing cyber risks”	By implementing ShadowPlex, financial institutions gain great visibility over cyber attacker activities within the infrastructure, enhancing the current defenses in addressing cyber risks.
Item 2 - “putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions”	ShadowPlex can provide real-time detection of incidents as adversaries attempt to navigate the network, or compromise existing systems, improving the responsiveness of existing Incident Response systems.
Item 3 – “ it is important to identify the inherent risks and the controls in place to adopt appropriate cyber-security framework”	One of the challenges in any security posture is identifying risks. ShadowPlex can be deployed alongside existing assets within any organization and show the activity of any cyber attacker before an asset is compromised. This level of visibility provides direct input on the level of risk, and ongoing risk the organization is exposed to. This visibility helps define

	and prioritize the appropriate framework policies that should be implemented.
Arrangement for continuous surveillance	
Item 6 - “continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats”	ShadowPlex is the industry’s only autonomous deception, designed to monitor cyber attacker activity regardless of their techniques. By continually adapting the solution to the activity of the network, ShadowPlex not only provides continuous surveillance, but also is ready for any type of attack whether it is known or unknown.
IT architecture should be conducive to security	
Item 7 – “The IT architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times”	Once deployed, ShadowPlex autonomously adapts to the infrastructure, ensuring that security measures are in place at all times, and in the locations needed.
Comprehensively address network and database security	
Item 9 – “It is essential that unauthorized access to networks and databases is not allowed”	ShadowPlex allows organizations to create deception assets including database servers, providing a new level of visibility that can immediately identify unauthorized attempts from cyber attackers attempting to gain access to critical database assets.
Cyber Crisis Management Plan	
Item 12 – “Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions”	ShadowPlex directly addresses the need for prevention of cyber-attackers, and immediate detection. Once deployed, you will be able to detect cyber attackers activity within the network infrastructure as soon as they begin their attack.
Item 12 – “Banks are expected to be well prepared to face emerging cyber-threats such as ‘zero-day’ attacks, remote access threats, and targeted attacks”	ShadowPlex is able to detect emerging cyber threats, and immediately identifies any attack techniques including zero-day and targeted attacks directly addressing the requirement. Acalvio has demonstrated the ability to detect the following attacks outlined in the requirement:

	<ul style="list-style-type: none"> • Ransom-ware / crypto ware • Destructive malware • Business email frauds including spam • Email phishing • Spear phishing • Whaling • Vishing frauds • Drive-by downloads • Browser gateway fraud • Ghost administrator exploits • Identity frauds • Memory update frauds • Password related frauds
<p>Item 14 – “banks need to report all unusual cybersecurity incidents”</p>	<p>For banks to be able to share cybersecurity incidents with other organizations, it is important to identify attacker activities as they occur – whether successful or prior to successful compromise. ShadowPlex is designed to detect attacker activities during all phases of an attack, providing details of the attack in multiple consumable formats that is readily shareable with other organizations.</p>
<p>Supervisory Reporting framework</p>	
<p>Item 15 – “ It has been decided to collect both summary level information as well as details on information security incidents including cyber-incidents”</p>	<p>ShadowPlex alerts include summary information, as well as details of the attack. The exported data can be easily converted into the required format as described in Annex-3</p>

3.1. Annex – 1: Baseline Cyber Security and Resilience Requirements

<p>Key Points Preamble: b. It is important to endeavour to stay ahead of the adversary. c. Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time. d. It is important to keep the vigil and to constantly remain alert.</p>	<p>Acalvio provides broad, real-time vigilance of adversaries at all stages of the cyber kill chain.</p>
<p>4.7 Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.</p>	<p>Using breadcrumbs and lures, ShadowPlex detects unusual activity in systems, servers and endpoints. Acalvio is also able to detect such activity if the activity results in attempted communication to Acalvio decoys.</p>
<h4>Network Management and Security</h4>	
<p>Item 4.9 - “Security Operation Centre to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities”</p>	<p>ShadowPlex can identify attackers across all phases of the cyber kill chain. Early detection during reconnaissance phases allows ShadowPlex to alert security teams to the presence of an attacker before any successful attack has taken place. These activities offer high fidelity alerts with no false positives, allowing teams to detect and remediate the attacker before any damage.</p> <p>Also, by leveraging our patented autonomous deception technology, ShadowPlex can offer decoy systems to attackers, which provides specific details in their intentions and attack techniques without sacrificing real assets.</p>
<h4>8. User Access Control/Management</h4>	
<p>Item 8.2 - 8.2 “Carefully protect customer access credentials such as logonuserid, authentication information and tokens, access profiles, etc. against leakage/attacks”</p>	<p>By implementing ShadowPlex with the endpoint tokens, you can detect when users credentials have been compromised by an attacker. Also, the core of the deception capabilities allows you to track all attacker activities, including usernames and passwords presented to any decoy. The usernames/passwords presented by attackers to decoys can be compared with real user accounts to determine which user accounts have been compromised before they are used against real assets.</p>
<p>Item 8.5 “Implement appropriate (e.g. centralized) systems and controls to allow, manage, log and monitor</p>	<p>Critical system administrator credentials can be monitored similarly as user credentials. By deploying critical asset decoys that replicate the real assets (minus the critical data),</p>

<p>privileged/superuser/administrative access to critical systems (Servers/OS/DB, applications, network devices etc.)”</p>	<p>ShadowPlex can easily detect when privileged/superuser/administrative accounts are being used to attempt to access the decoy. Details of the access attempts include the passwords presented so that security teams can easily identify if critical account passwords have been harvested, allowing them to remediate the accounts before any damage is done.</p>
--	--

13. Advanced Real-time Threat Defence and Management

<p>13.1 “Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise”</p>	<p>Malicious code can be injected almost anywhere in the enterprise. Perimeter, DMZ, or otherwise limited coverage is not sufficient to meet this requirement. ShadowPlex is designed to be deployed broadly across the estate, and therefore provides a superior defense against malicious code execution.</p> <p>ShadowPlex is designed not only to identify active cyber attackers within an infrastructure, but to redirect malicious code/payloads into decoy systems. This capability redirects malicious code into decoys that not only prevent the installation and spread, but provide valuable insight into the attack intentions.</p> <p>ShadowPlex ensures that as attackers seek out new systems, they will be presented with dynamically created decoys that ensure protection of critical assets while preventing the spread of malicious content across multiple points within the enterprise.</p>
--	--

<p>13.2 Implement Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralised management and monitoring.</p>	<p>ShadowPlex delivers behavior detection capability across the environment, including all system types defined in 13.2. ShadowPlex is agnostic to the source of the compromise: As soon as the compromise attempts to move laterally, ShadowPlex will detect it. Furthermore, the solution centralises all management and monitoring.</p>
---	--

15. Data Leak Prevention Strategy

<p>Item 15.1 – “Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and</p>	<p>When deploying ShadowPlex, you can create decoy assets and decoy data that impersonate real assets and data. By impersonating data assets with fake content, you can create a</p>
--	--

<p>customer data/information”</p>	<p>realistic environment for attackers which will alert you to their presence, as well as which data is being accessed/retrieved/encrypted.</p>
<p>Item 15.2 – “This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline”</p>	<p>ShadowPlex includes endpoint tokens, which enable you to identify when these files are being accessed by adversaries.</p>
<p>19. Incident Response & Management</p>	
<p>Item 19(c) – “Contain the level of cyber-attack by implementing shielding controls/quarantining the affected devices/systems”</p>	<p>ShadowPlex implements decoy systems alongside real assets and lures attackers to these decoys before they breach the real asset. This decoy system provides instant identification of an attack, and can keep the attacker occupied protecting the real systems.</p> <p>In addition, ShadowPlex can “move” the decoy into a network of other decoys giving the attackers the impression that they have additional targets, all the while moving them into a quarantine network.</p>
<p>19.2 Have written incident response procedures including the roles of staff / outsourced staff handling such incidents; Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication & co-ordination with stakeholders during response;</p>	<p>ShadowPlex should be included in the response procedure for the purpose of situational awareness. In addition to providing basic information about the attack, its ability to engage the attacker allows it to develop intelligence about the attacker's identity and techniques.</p>
<p>19.6 Resilience Testing: (e) Contain the level of cyber-attack by implementing shielding controls/quarantining the affected devices/systems.</p>	<p>ShadowPlex contains cyber-attacks through obfuscation: The solution masks the presence of production assets, retarding the ability of attacks to propagate.</p>

3.2. Annex – 2: Setting up and Operationalising Cyber Security Operation Centre (C-SOC)

Introduction	
<p>Item 3 – “Constant and Continuous monitoring of the environment using appropriate and cost effective technology tools”</p>	<p>ShadowPlex has been designed to continuously monitor entire network infrastructures and determine when adversaries are present, presenting them with decoy systems before they identify and compromise real assets. ShadowPlex is industry’s only autonomous deception solution is able to dynamically adjust to the network and assets without requiring ongoing updates.</p>
Cyber SoC: Points to be considered	
<p>Item 1 – “necessarily take into account proactive approaches rather than reactive approaches and have to also address possible unknown attacks. For example, zero day attacks and attacks for which signatures are not available have to be kept in mind”</p>	<p>ShadowPlex is designed from the ground up to identify attackers without requiring pre-definition of their attack tactics or methods. The ability to deliver an autonomous deception infrastructure that is automatically tailored to the environment ensures all networks and assets are covered from cyberattacks. Each decoy or endpoint token will alert to the presence of any attacker including zero day attacks, and attacks that have known signatures (although signatures are not needed for detection from Acalvio).</p>
<p>Item 2 – “The Cyber SoC has to take into account proactive monitoring and management capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytics”</p>	<p>ShadowPlex’s autonomous deception solution is to continuously monitor the network, proactively seeking any attacker activity across the entire cyber kill chain. Once detected, the security team is immediately alerted while the solution keeps the attackers occupied safeguarding real assets from compromise.</p>
<p>Item 4 - The systems that NEED to be put in place as a part of the Cyber SoC requires the following aspects to be addressed.</p> <ul style="list-style-type: none"> • Methods to identify root cause of attacks, classify them into identified categories and come out with solutions to contain further attacks of similar types. • Incident investigation, forensics and deep packet analysis need to be in place to achieve the above. 	<p>ShadowPlex provides all three NEEDED systems: root cause analysis (through attacker engagement and full stack decoys); incident forensics and packet analysis (deep engagement), and honeypot services (variable interaction decoys). ShadowPlex addresses these aspects as follows:</p> <ul style="list-style-type: none"> • Each attack is identified with details on the source of the attack, as well as the methods deployed by the attacker. This data highlights the root of the attack, and delivers comprehensive forensics so that future attacks can be prevented at the source, or by the attack profile.

<ul style="list-style-type: none"> • Dynamic Behaviour Analysis. – preliminary static & dynamic analysis and collecting Indicators of Compromise (IOC) • Analytics with good dash board, showing the Geo-location of the IP's • Counter response and Honeypot services 	<ul style="list-style-type: none"> • Detailed forensic data on the attack, alongside packet data is preserved for detailed analysis • All behavior of the attack is recorded, including commands attempted, and payloads utilized, which is compiled as comprehensive IOC's • All attacks are recorded with internal system identification (IP addresses), as well as any external communications with GEO location data • The entire solution is designed as a counter response system, leveraging dynamic/autonomous honeypots that lure attackers in and isolate them for the duration of the attack.
<p>Expectations from SoC</p>	
<p>“Ability to know who did what, when , how and preservation of evidence”</p>	<p>ShadowPlex provides real-time insight into the security posture of the bank using the best possible method: A broad view of actual attack activity across all internal assets. Unlike other detection systems, ShadowPlex directly interacts with cyber attackers, allowing them to believe they are interacting with a real asset. By allowing attackers to attack ShadowPlex decoys instead of real assets, the solution is able to record all activity, including knowing the source of the attack (who), what techniques they are doing and intention of the attack (what), and accurately record when the attack took place (when). Each attack is recorded from initial reconnaissance to completion, preserving valuable evidence for security team forensics.</p>
<p>Technology Issues: First step is to arrive at a suitable and cost effective technology framework designed and implemented to ensure proactive monitoring capabilities aligned with the banking technology risk profile and business and regulatory requirements. - Fourth step is to have tools and technologies for malware detection and analysis as well as imaging solutions for data to address the forensics requirements</p>	<p>One of the biggest challenges in cyber-security is cost-effectiveness. There are many options that are theoretically possible but cannot be deployed in a cost-effective manner. ShadowPlex's Deception Farm approach (including our pricing model) is built for cost-effective scale. Through centralization and projection, combined with variable interaction decoys, Acalvio can deliver cost-effective proactive monitoring capabilities across the estate.</p>
<p>“Integration of various log types and logging options into SIEM”</p>	<p>ShadowPlex supports export of logs to any SIEM [Splunk, QRadar, ArcSight, LogRhythm, RSA Netwitness, NetMonastery,</p>

	etc.]
--	-------

3.3. Annex – 3: Template for Reporting Cyber Security Incidents

<p>Key Points Preamble: b. It is important to endeavour to stay ahead of the adversary. c. Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time. d. It is important to keep the vigil and to constantly remain alert.</p>	ShadowPlex provides broad, real-time vigilance of adversaries at all stages of the cyber kill chain.
---	--

Template for reporting Cyber Incidents (Annex 3)

<p>5. Root Cause Analysis(RCA):</p>	
Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident	ShadowPlex provides deep engagement of the attacker's identity, techniques and motives to drive root cause analysis.

Cyber Security Incident Reporting Form (Annex 3)

<p>5. Types of Threat/Incident</p>	ShadowPlex provides rich information on the type of incident (e.g. malware, intrusion, APT), which is necessary to answer this question.
<p>7. Please provide details of the incident in the box below. How was the incident first observed/sighted/detected?</p>	As a broad line of detection, ShadowPlex can serve as the first point of detection.
<p>8. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include: - Location, purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc.) running on the systems/ networks, etc.</p>	As a broad line of detection that includes detailed traffic analysis, ShadowPlex can provide details pertaining to the scope of the incident: Which subnets and systems are potentially affected.
<p>10. Does the affected critical system(s)/ network(s) have potential impact to another critical system/critical asset(s) of the bank?</p>	ShadowPlex provides both the scope of the incident, and the methods and internal targets used, the solution can determine which additional critical systems are at risk.
<p>13. What is the earliest known date of attack or compromise? (Tick 'checkbox' if</p>	ShadowPlex provides a complete audit trail of the attack, making it trivial to determine the earliest date of compromise.

unknown)	
14. What is the source/cause of the incident? ('NIL' OR 'NA' if unknown) Click here to enter text.	ShadowPlex provides deep engagement of the attacker's identity, techniques and motives to determine the source of the incident.
Attack Vectors: E1. Did the bank locate/identify IP addresses, domain names, related to the incident	Depending on the type of attack and level of engagement, ShadowPlex can determine the external addresses or domains related to the incident.

“The Cyber SoC has to take into account proactive monitoring and management capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytics.”

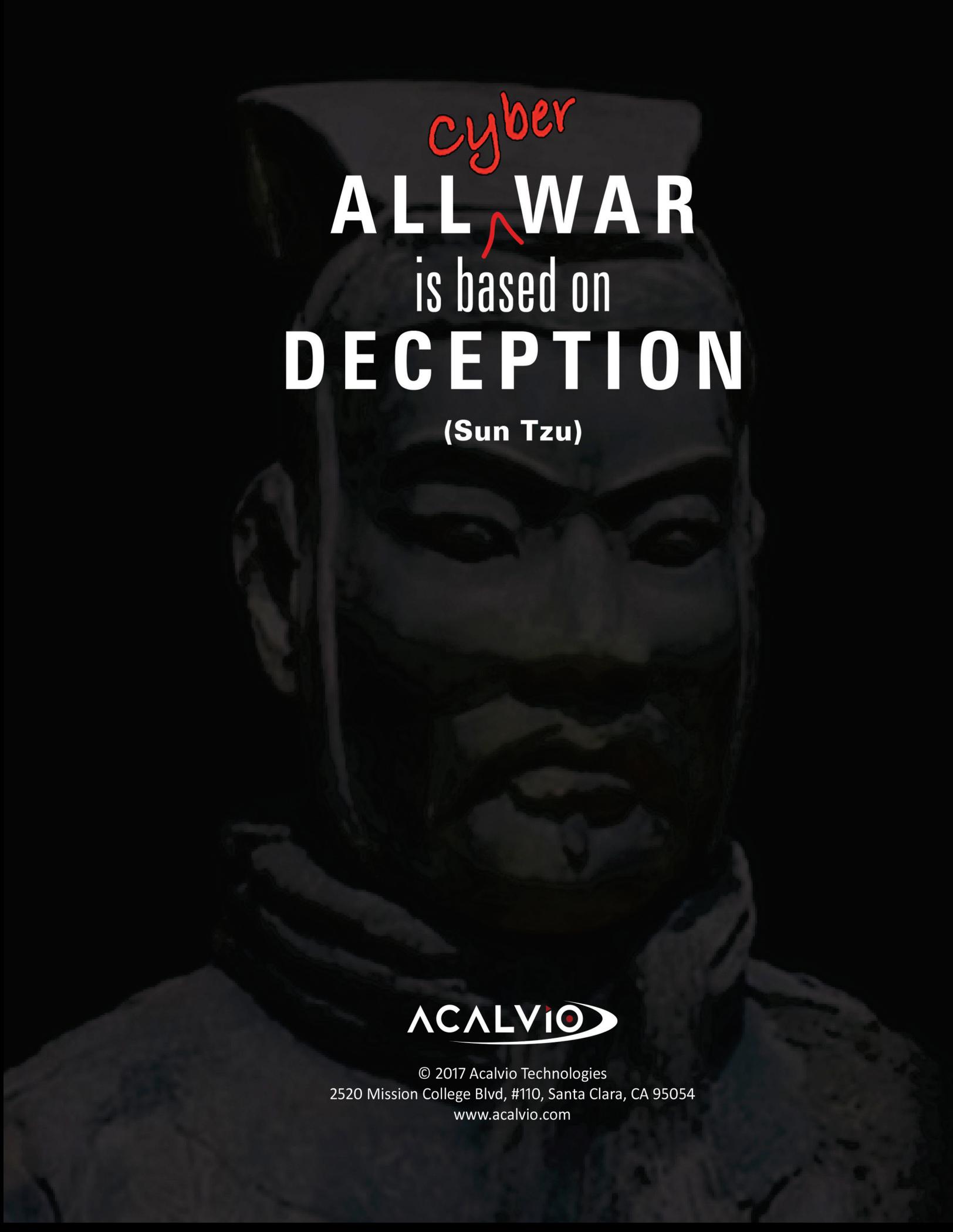
Cyber Security Framework in Banks, RBI, 2016

4. Summary

The cybersecurity guidelines issued by the Reserve Bank of India in 2016 serve as a stark reminder of the need for robust cyber threat detection and response. Although the RBI released extensive IT security guidelines in 2011, it felt compelled to update its guidance in part because the original advisory didn't sufficiently address the need for post-breach capabilities. ShadowPlex is uniquely suited to support the new threat detection guidelines, as part of a bank's broader cyber security strategy.

About Acalvio

Acalvio provides Advanced Threat Defense solutions to detect, engage and respond to malicious activity inside the perimeter. The solutions are anchored on patented innovations in Deception and Data Science. This enables a DevOps approach to deploying enterprise-scale pervasive deception, with low IT administrative overhead. Acalvio delivers comprehensive threat intelligence by integrating with other 'best in class' solutions in the security industry, enabling customers to benefit from defense in depth; reduce false positives; and derive actionable intelligence for remediation. The Silicon Valley based company is led by an experienced team with a track record of innovation and market leadership and backed by marquee investors. For more information, please visit www.acalvio.com



cyber
ALL WAR
is based on
DECEPTION
(Sun Tzu)

ACALVIO

© 2017 Acalvio Technologies
2520 Mission College Blvd, #110, Santa Clara, CA 95054
www.acalvio.com