*Federation of Business Disciplines Journal*

Volume 16, 12-26

**TELL ME SIMPLY: WHAT IS YOUR CYBERSECURITY POSTURE AT THE MOMENT?**

**Rashid Manzar**

*Verizon, Atlanta*

Alpharetta, GA 30022

USA

**Rajat Mishra**

*Stephen F Austin State University*

Nacogdoches, TX, 75962

USA

**ABSTRACT**

Organizations struggle to keep their cyber security posture apt in order to meet regulatory requirements, compliance, and privacy & protection needs of their digital assets. Many well-established frameworks such as NIST CSF 1.0 and 2.0, ISO 27001, and ISO 27002 provide guidelines to organizations of all sizes, to implement controls in order to reach desired security objectives. These frameworks provide granular details for implementing technical controls under various functional units described within them. They offer assessments which can be used to fill gaps that are detected in reaching a desired security posture. However, a theoretical lens for the assessment of cyber security posture is also warranted that can help understand and study cyber security posture as a moving target similar to periodic assessment of technical controls that IT organizations setup. The current paper fills this gap by analyzing the actors and the status of protection of the elements of digital assets and introduces a simple two-by-two framework.

**Keywords:** Cyber security posture, compliant, violated, compromised, secured, two-by-two model

**INTRODUCTION AND LITERATURE REVIEW**

Frameworks such as NIST Cyber Security Framework (CSF), ISO 27001, and 27002 come very handy in guiding any organization in establishing their cyber security profile (Pascoe, 2023). Practitioners and IT organizations benefit immensely by implementing guidelines from those frameworks and potentially avoid security events (Scofield, 2016). Organizations model and monitor threat to safeguard their IT assets. Threat Modeling has been universally employed by IT organizations to study and model threat landscape where hackers try to penetrate IT systems while organizations prepare defense mechanisms by deploying necessary tools, technologies and personnel (Muckin & Fitch, 2014). In the current paper, we provide theoretical as well as practical guidance to assess cyber security posture. Prior research has used quadrant diagrams to study malicious IT (bad actors) and virtuous IT (good actors) (Liang & Xue, 2009). We developed our research framework building on the quadrant diagram by considering two axes, one axe using good actors and bad actors as two levels of actors. The other axis of our framework utilizes the two levels of IT security posture, one being a “not-penetrated” or protected state (a desired state to be in) and another being the undesired or penetrated end state. It’s important to note that good and bad actors are not just individuals, but they can be hardware devices or software automated tools as well.

Cyber-security is much like an arms race where weapons and mechanism of defense are constantly in competition with each other where bad actors want to illegitimately gain access to digital assets through cyber-attacks. We begin by identifying the elements of digital infrastructure assets which are always at the risk of being compromised. These elements have been identified in NIST CSF under the functional heading of “protect” (Framework, C. 2021) and also through the confluence of leading companies and department of defense ([DoD](about:blank) Cyber Security Division, 2023; Cloud Security Technical Reference Architecture Cybersecurity, 2022; The Microsoft Cybersecurity Reference Architectures (MCRA); Security of the AWS Infrastructure, AWS, 2024).

**Table 1**

**Elements of cyber security which may face the risk of being attacked**

|  |  |
| --- | --- |
| Elements of cyber security | Definitions of cyber elements in an organizational context |
| Identity and Access Management | A person, a user, a role or a federated-identity that has access rights to computing resources |
| Physical Assets | A piece of hardware asset directly or remotely accessible or a building housing computing resources |
| Infrastructure platform software | A piece of software that is used as platforms on which organizations build their own customized applications |
| Application | A piece of software that is developed or procured or available from free sources such as open-source software |
| Network | A technology that is responsible for connecting computing resources to inside and outside of an organization |
| Databases | A technology that manages the storage, manipulation and retrieval of digital assets of an organization |
| People | An employee, a consultant or a contingent worker who are part of organization |
| Social | An enabling technology that links an organizational identity to the outside of an organization in a public domain |
| Policies | Organizational rules of engagement with people, system, organizations to do business in a safe and secured way |

As important as identifying the cyber elements are, identifying the actors are equally important - actors that act in the interest of the organizations they are employed with, and actors, that are adversaries (domestic or foreign) and want to harm the organizations and their assets they target to attack (Sabillon et al., 2016). Various threat agent archetypes have been studied in the industry and have been broadly identified as hostile and non-hostile (Casey, 2007). With this threat archetype library, organizations are faced with two actors. On one side, there are actors who works on behalf of an organization and in the interest of organization to protect business use-cases of IT (virtuous IT). On the other side, there are those actors whose intent is malicious and are engaged in abuse-cases and their purpose is to exploit any vulnerabilities that they can use to their advantage (Juuso, 2019; Uceda-Vélez & Morana, 2015). In the cyber security world, organizational actors are tasked to protect their IT systems to make sure that the IT systems are well protected physically and virtually. They can be site inspectors, load runners, disaster recovery planners, code scanners (static, dynamic and runtime), ethical hackers or penetration testers. They are good actors and often wear several hats to ensure the security of the IT systems and IT assets. They are popularly called blue and red teams. Red teams are those ethical hackers who help test an organization’s defenses by identifying vulnerabilities and launching attacks in a controlled environment. Red teams are opposed by defenders called blue teams, and both parties work together to provide a comprehensive picture of organizational security readiness (NISTIR 7622, 2012; Yaqoob et al., 2017). Besides these teams, organizations use automated tools for scanning code or testing their applications or employ run time protection mechanisms or do stress testing. Notable scanner types technologies are Static Application Security Testing Tools (SAST), Dynamic Application Security Testing (DAST), Runtime application self-protection (RASP), and Interactive application security testing (IAST) (Ashtari, 2024; Čisar & Čisar, 2016; Mughal, 2018). SAST is a white-box testing method where security team gets the access to the code base and vulnerabilities are detected when code scanner scans through the code. IAST is a black-box (no access to the code) testing method for dynamic application security that highlights and analyzes vulnerabilities during application runtime when they are live. DAST is a black-box testing methodology for running applications to highlight external vulnerabilities. Runtime application self-protection (RASP) is another advanced security solution integrated into an application or runtime environment to highlight and thwart security attacks as and when it happens.

On the other hand, there are hackers or hostile agents who are engaged in criminal activity and aim to gain access to some organizations and its resources illegally and exploit any vulnerability to their advantage and we call them bad actors or threat agents. These bad actors are oftentimes very resourceful and pose persistent threats (they may stay dormant within network until they find a ripe time for exploitation) in order to gain access or to elevate their privilege if they already have gained access. Some of these hackers are nation or state sponsored and are called nation-state actors and they are employed by foreign governments to disrupt or compromise target governments, organizations or individuals, valuable data or intelligence (Hinck & Maurer, 2019). The other bad actors are insiders who look for exploiting vulnerabilities often times for monetary gains since they already have access to the systems (Hunker & Probst, 2011). Besides these, there are automated tools, and bots who can pose constant threat of external attacks on organizational infrastructure (Lange & Kettani, 2019). These tools are often times employed by penetration testers themselves in a controlled environment. GitHub, which is one of the most popular code repositories (Borges et al., 2016; Jiang et al., 2017) provides thousands of readymade utilities that can help generate payloads of varying intensity or can even be forked to tailor organizational needs for testing against hacks. The table 2 presents the good and the bad actors an organization is faced with.

**Table 2**

**Good and Bad Actors**

|  |  |
| --- | --- |
| Good actors (On behalf of their organizations) | Bad actors (who act against target organizations) |
| Ethical Hackers | Insiders with malicious intent |
| Property Managers/ Site Inspectors / DR Planners | Nation-state actors |
| Network and Database scanners | Automated Tools and Scanners |
| Static Application Security Testing (SAST) Tools | Adversarial threats and Advanced Persistent Threats |
| Dynamic Application Security Testing (DAST) Tools | Spy vendors |
| Runtime application self-protection (RASP) | Disgruntled employees |
| Interactive application security testing (IAST) | Data miners |

A desired security posture of an IT asset is a state in which all identified elements in table 1 are in compliance with the security policies of an organization and in adherence to standards and regulatory requirements and laws for the respective industries. Organizations can meet compliance by establishing risk-based controls that protect the confidentiality, integrity and availability (CIA) of information (Sulaiman et al., 2022; Cram et al., 2017; Miller, 2023). However, compliance only guarantees that all policies are enforced, it does not guarantee protection against unseen and unknown threats. The desired state in terms of cyber security is the one in which all the elements of cyber systems are compliant and protected against all current attack vectors. This is tantamount to say that the system is well defended. Non-compliance happens when there are known gaps from reaching the compliance goals. This would mean that there are known vulnerabilities that needs to be remedied and until it is remedied, such assets are non-compliant and in violation of established security policies and are prone to be compromised. (Marotta & Madnick 2021; Portman & Carper 2018; Nasir et al. 2019). A compromised system takes away the guarantee of confidentiality, integrity and availability (CIA Triad) from the cyber systems. Data breaches (exfiltration of data) potentially due to non-compliance amongst other reasons have been reported time and time again (Al-Mukahal & Alshare 2015; Herath et al. 2023; Karyda & Mitrou, 2016). We will discuss individual elements mentioned in Table 1 and their role in protecting IT assets.

**Identity and Access Management (IAM)**:

Identity is an account identifier that does the handshake with the computing resources. This is the most fundamental entity that once compromised, it is left to be abused. Identity can be a user, a role or a federated identity or merely a time-bound token. Users of an organizations are managed by active directory or some type of organizational authentication process and users outside of an organization who legitimately wants to gain access of some systems are often times are allowed to use their verified digital passports such as a Gmail, or a LinkedIn, or a Facebook, or a twitter account (a.k.a federated identities). The idea behind IAM is stated as “who-can-access-what”. (Hovav & Berger 2009) Provisioning an identity, authenticating afterwards and the authorization process is one of the most challenging and complex tasks for any organization. Fortunately, few very well-established methodologies for Identity and Access Management (IAM) exist that help organizations to make sure that they bullet-proof the identity provisioning. Important implementations in this IAM area are Role Based Access Control (RBAC), Single Sign On (SSO) and Privileged Access Management (PAM) (Mughal 2018). The latest technological advancement in bullet proofing an identity is provided by Zero-trust framework that helps IAM create, maintain, and manage identities in an automated fashion (Rose et al. 2020).

However, an idetity is not something that stays immune to any abuse. Broken authentication have moved up in the ranking of OWASP top 10 vulnerabilities (Pandya & Patel 2016) in recent years. The result of a broken or forged identity acquired by a malicious user can turn a secured system into a compromised system. A stolen identity by a malicious outsider or criminal actor can ex-filtrate and steal valuable private information and render an organization or end-users into a compromised entity. Thus, identity and its management therefore has the possibility of moving from a protected state to a penetrated state rendering information user from a secured state into a compromised state and when this happens at the scale of an organization, it can render an organization from a secured state to a compromised state.

Once identity is compromised, it will require organizations to take corrective actions to come back to defended status after isolating the compromised identities and making sure that compromised identity is no longer usable by a threat actor, internal or external. The penetration testers such as red and blue teamers once again will need to make sure through testing that all identities are properly authenticated and authorized and with their certifications, the information system can go back to a compliant state, achieving an overall secured posture. If ethical hackers (good actors) can still penetrate through the system from their testing procedures in good faith, then the information system will fall in the violated state, and furthermore, if threat actors can gain access to the system then it moves to a compromised state and can even be breached. Security teams must continuously monitor the identity. A compliant system generally is well guarded and protected against known bugs and vulnerabilities. However, there is no protection for compliant system when it comes to zero-day attacks as there is no patch yet available from hardware or software vendors or from open-source communities (Ahmad et al. 2023) and this puts a fully compliant systems to fall in the violated category even though it may not have yet been exploited and breached by bad actors.

**Physical Security**

An organization has countless physical computing assets that need to be safeguarded. Datacenter, hardware, storage areas, network devices, endpoints, personal devices all need to be physically protected against infiltration by any intruders. Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and even spilled coffee) (Moses & Rowe 2016). Good actors assigned to physical security (as in Table 2) have to make sure that infrastructure is protected and remain operational by employing organizational approved means (resources, tools and technologies). Bad actors can cause property damage, can infiltrate heavily guarded data centers and unattended locker rooms, can install plug and play devices or key loggers, and steal equipment from the data centers. Therefore, a fully compliant and defended physical infrastructure runs the risk of being violated or breached rendering the infrastructure from a secured state into a compromised one.

**Application Security**

An organizational infrastructure develops their own applications or purchases vendor based applications or employs open source software to achieve their business goals. Every application goes through cycles of releases in its life cycles through change management processes. These application code developed in-house or used as a component in their applications or employed as an API from external sources always often time will be detected with bugs and vulnerabilities. Common vulnerabilities such as OWASP TOP 10 (Rose et al. 2020) or common vulnerability and exposures (CVE) (Mann & Christey, 1999; Martin, 2019) that are published by security monitoring entities must be tracked by every organization to continuously remediate vulnerabilities. Several organizations use static application security testing tools (SAST tools such as Fortify, Checkmarx, SonarQube) which detect code vulnerabilities and offer remediation steps (Yang et al. 2019; Pittenger 2016). Open source vulnerabilities are also detected by SAST tools (such as Black Duck). An organization can stay compliant as long as they patch all known vulnerabilities that were detected by code reviewers or code scanners or run-time scanners. And they can stay defended as long as malicious users can’t exploit them. However, code changes continue to have exposures from unknown bugs and zero-day vulnerabilities for which there is no patches yet. These can change the security posture of an organization from being violated to even breached, if it can be exploited by malicious actors. Therefore, a fully compliant and defended application security posture runs the risk of being violated or even compromised rendering the application security state from a secured state into a compromised one.

**Infrastructure Platform Security**

Besides protecting physical security, every organization has to be vigilant on software or platforms that they purchase or subscribe it under Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) cloud subscription agreements. These include operating systems, virtual machine images, containers, utility software such as antivirus software, database system software, office desktop software such as Microsoft Office and GSuites. (Alhazmi & Malaiya 2008). These platform software themselves go through cycles of releases and patches/fixes/service packs that must be applied in the recommended time frame by the corresponding platform vendors. Organizations continue to harden these platforms on a continuous basis. However, these platform software continue to have exposures from unknown bugs and zero-day vulnerabilities too and must be scanned from time to time for vulnerability detection. If vulnerabilities are detected, it can change the security posture of an organization from being violated to compromised or even breached, if it can be exploited by malicious actors. Therefore, a fully compliant and defended platform security posture runs the risk of being violated or even compromised rendering the platform security state from a secured state into a compromised one.

**Network Security**

Corporate networks are a complex mesh of computing devices and software that facilitate inter and intra connectivity amongst computing devices. These include setting up of VPNs, NAC solutions, routers, switches, firewalls, DMZ, WAF, IDS, IPS, DDoS protection, SSL interceptors. (Mughal 2018). As much as the network facilitates business, they can also become the first line of attack by bad actors. Therefore, implementing security systems at the network boundaries boost up the organizational perimeter security and helps organizations deter attack and defend themselves proactively. Thus, securing network protects organizations from cyberattacks. Many organizations use network scanners (in good actor’s faith) such as Tenable, Qualys, and Rapid7 to continuously monitor their network against vulnerabilities. On the other hand, bad actors continue to find innovative ways that can be employed to penetrate through networks and oftentimes they are successful as we hear in news about breaches. This puts a fully compliant and secured network to land in a compromised domain until a fix is applied and networks are hardened again to become compliant and able to be defended against threats.

**Database Security**

Of all the digital inventory that an organization owns, data is their currency. This digital asset unlike others relatively stays longer in its original form and sometimes outlive tenure of its owners than rest of the elements that we mentioned above for business and regulatory reasons that needs to be complied with as to how to insure data protection and privacy. Amongst most notable regulations known today are GDPR, CCPA, HIPAA, DSS PCI (Miller, 2023) and most business domains fall under some regulatory obligations that they must adhere to. For example, google maintains email as long as they can and probably none of us have seen emails being purged from our google accounts and it will stay even if the owner of emails dies. The attack on data is incessant and organic. Data breaches have almost become a daily event. Top tier organizations such as ForgeRock, IBM and Verizon have published separately very extensive reports on data breaches (Ponemon Institute, 2020; Forgerock 2019; Team, V. R., 2015). Providing security of data in transit and data at rest is an organizational survival need. Most IS use TLS for data in transit and AES encryptions for data at rest (Malik & Patel 2016). Cloud providers also implement their own flavor of encryption that guarantees security through transit and at rest. A data breach can wipe out an organization from existence and put executives in legal jeopardy. Yet, this is still one of most heard news on a day to day basis. Many database monitoring tools (such as IBM Guardium, and Imperva) provide logging and monitoring of database activities round the clock. In Spite of all the monitoring things go wrong, and systems at times become non-compliant and are in violation of policies and on top all this, newer regulations add complexity to existing security gaps. When a new clause or new laws are added many organizations cannot comply with them instantly and stay in violation for some time and become prone to be breached. This can turn an organization from an overall secured posture to a compromised posture in managing data.

**Employee Awareness and Training**

With the complexity of cyber physical systems growing every day, it is extremely hard to cope with the newer techniques and threats that are being employed by bad actors. This has put cyber security amongst the fastest growing field and demand for cyber security certified professionals are ever increasing (Furnell et al. 2017). Employee’s awareness of secure coding and how to deal with spammers and phishers is essential for protecting digital system (Li et al. 2019; Aldawood & Skinner 2018). Employees are social engineered and phished and unfortunately due to tremendous shortage of personnel available in the cyber security area, an untrained or less trained professional may unknowingly give out valuable private information through phishing and can throw a fully compliant organization or a system into an organization or a system in violation or may even become prone to be breached. Fixing such awareness weaknesses through employee continuous training and certifications may help regain a secured posture by becoming compliant and be defensible against bad actors.

**Social Domain Security**

In Web 2.0 and Web 3.0 era, there is hardly any organization left that does not maintain its social presence. If not careful, employees through public interactions or through public forums can inadvertently put private information related to the organization's business confidentiality. Open source intelligence (OSINT) is becoming widely popular where various publicly available information becomes sources for exploitation by threat actors. (Carley et al. 2018; Glassman & Kang 2012). Protecting vital information to fall in the public domain is essential for business survival and revealing any private and confidential information even inadvertently can be a violation and breach of information from the angle of stakeholders. Damages done in the social domain are generally long lasting and oftentimes irreversible and regaining a secured posture becomes a long shot.

**Policies**

One of the important tenets of cyber security is to manage risk since gaining any protection against threats has to be economically viable for corporations to sustain. (Lubua & Pretorius, 2019). Depending on financial costs, organization can triage risk priorities since no organizations can eliminate all possible risks due to financial infeasibility of doing that. Therefore, organizations manage risks through triage by setting up policies and procedures. If these policies are not implemented and there are gaps left in policy implementations as they are laid out by organizational leaders, it puts an organization in violation and therefore at risk to be breached and compromised. By putting policies in place, organizations maintain their secure postures.

**MODEL DEVELOPMENT AND PROPOSITIONS**

The above background helps us formulate a security framework that helps us understand a constant struggle from being in a state of compliance and defended to fall in a state of violation and being breached. We consider a two-by-two matrix where we consider actor archetypes (good and bad actors) and protection status of being protected (not penetrated) versus being penetrated to study this phenomenon. Earlier studies have used two-by-two models to study competing organic phenomenon graphically, generally one axis measuring strength and weakness of the agents and other axis measuring strength or weakness of the act itself. One of the most notable study is Gartner’s magic quadrant (Sallam, et al. 2011) in which the magic quadrants help us quickly ascertain how well technology providers are executing their stated visions and how well they are performing against Gartner’s market view. In this research, we borrow from the quadrant logic to use the strength and weaknesses of penetrative ammunitions of an actor (mentioned in Table 2) to intrude versus the strength or weakness of the individual element of the Table 1 (the ability to actually intrude or gain access). Figure 1 shows the four quadrants and their meaning in terms of security postures. We describe four states of security postures mentioned in Figure 1 in Table 3 (compliant, secured, violated, and compromised) based on how successful the good actors find themselves in exploiting vulnerabilities and similarly how successful the bad actors find themselves in exploiting the vulnerabilities.

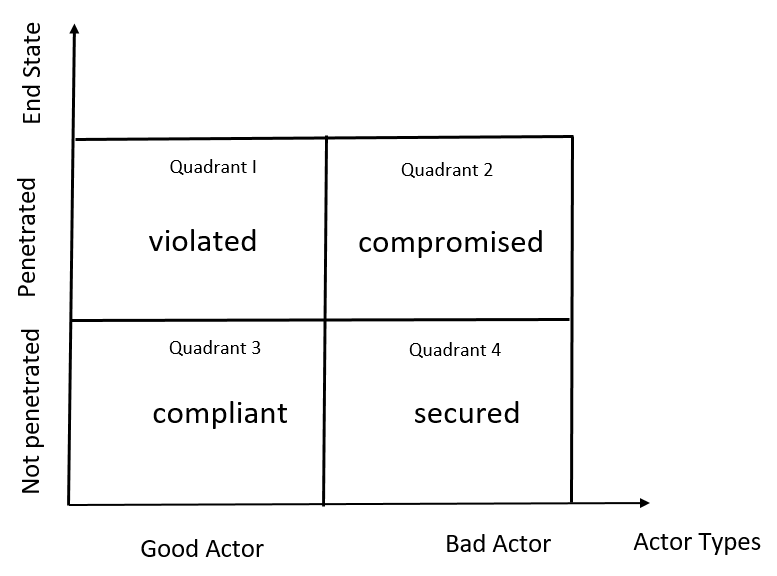
**Table 3**

**Various States of Security Postures of Individual Elements of Cyber Security**

|  |  |
| --- | --- |
| **Security posture** | **Definitions of various state of security postures** |
| Compliant | Being compliant means, all known vulnerabilities are either remediated or have an approved exception from risk management team not to seek remedy. It does not mean that every vulnerability has been remediated, instead, it means that given an organization’s appetite for assuming risk all vulnerabilities have been addressed. Thus it is risk-based remediation for compliance. |
| Secured (Defended) | When malicious actors are unable to break in and exploit the asset, we call it secured or defended against threat actors. |
| Violated | When certain vulnerabilities are found and remains unpatched and has not been remediated and are within the period granted for remediation, we call those assets are in violation. |
| Compromised (Breached) | When vulnerabilities become exploited by malicious actors and an organizational assets are prone to be ex-filtrated out to unauthorized parties then it is compromised and can possibly be breached. A data breach occurs when unauthorized parties infiltrate computer systems, networks or databases to gain access to confidential information. |

Table 1 lists individual elements of cyber security and Table 3 lists their possible state of security postures, however, an organization’s IT is comprised of complex mix of those individual elements. Most fundamental of organizational entity may be a business unit or just one application through which an organization exists or known as a business. Good or bad actors whether a person or an automated tool follow a playbook through which they organize their security testing or exploitative forces. Just like body of knowledge differs from one teacher to another, good actors/tools can have variations too. Two different tools or two security testers are not alike. Two different bad actors also may have different fire power of penetrative ammunitions and skills to discharge malicious payloads. However, as much as a playbook (procedure) is followed, the outcome (standardized metrics for vulnerability assessment) can be summed up from all penetration tests of individual elements or penetrative power of bad actors. Therefore, to protect against cyber security mishaps, a sum total of protection of those individual elements that make up an application are needed to be assessed. Therefore, we propose the following:

**Figure 1.**

**Good and Bad Actors versus their ability to penetrate**

**Proposition** 1: Compliant: An IT application can be considered to be compliant when all good actors responsible for penetration testing an application following the procedural steps are unable to penetrate through the application.

**Proposition** 2: Secured: An IT application can be considered to be secured when all bad actors responsible for penetrating an application are unable to penetrate through the application and fail to gain access to do malicious activity.

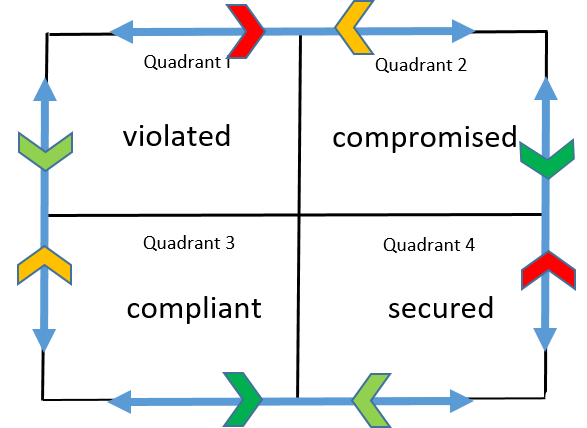
**Proposition** 3: Violated: An IT application can be considered to be in violation (violated) when all good actors responsible for penetrating an application are able to penetrate through the application and can prove that the application allowed unauthorized activity.

**Proposition** 4: Compromised: An IT application can be considered to be compromised or breached when all bad actors responsible for penetrating into an application are able to penetrate through the application and gain access to do malicious activity.

As discussed under various elements of cyber security above, the state of cyber security continues to be in a cyclical shift. That means there is no entitlement to enjoy for long for any organization. Thus, security posture is a moving target from any of the state to any other state such as from being compliant to secured and vice versa, from being secured to compromised/breached and vice versa, from being compromised to violated and vice versa, and from being violated to compliant and vice versa. This continuous flux in security posture has been depicted in Figure 2.

**Figure 2**

**Constantly changing security posture from one state to another**



**IMPLICATIONS**

Industry uses cybersecurity frameworks that provide them guidelines irrespective of size of organizations to manage and reduce cyber security risks. The frameworks are further organized into functions to facilitate the tasks needed to be accomplished in order to reach some desired level of security postures. For example, NIST CSF v1.0, and v2.0, ISO 27001, and, ISO 27002 provide many functional units under their framework that organizations need to tackle and address security gaps. They provide implementation guidelines broadly. The goal of this academic research is to provide an abstraction to academicians much like an industry frameworks provides to practitioners. Our framework is very intuitive and provides an abstraction of interaction between type of actors and state of protection on which cyber security posture can be understood. Although this research is offering a theoretical angle, the intended outcome bears the same goal similar to industry frameworks, which is, understanding the overall cyber security posture and prepare interventions accordingly. Like practitioners delve deeper into granularity of functions, and categories and subcategories of frameworks, academicians try to understand factors in the model and their direct and interaction effects of those factors at different level. In our case, the direct effects are the strength and weakness of elements of cyber security per se, while indirect effects originate from the interaction of strength and weakness of actors and the strength and weakness of cyber elements themselves. An empirical study with survey-based research by developing scales depicting the strength of actor types and strength of individual cyber elements would be a good step to see the benefits of the proposed framework.

Our framework suggests that cyber security posture is not a fixed or an achieved goal, it is rather a moving target which struggles to maintain its position from the most privileged state of being secured to the most undesired state of being compromised or breached. Quadrant I of Figure 1 depicts a scenario, where good actors through their testing processes of security controls could penetrate the IT system or an application and thus in a state of violation. Quadrant 2 depicts a scenario where bad actors could successfully penetrate through security controls and breached the system. Quadrant 3 represents that the good actors could not be successful in penetrating through the security controls with all the penetration tools they had at their disposal provided by the organization and thus are compliant. Quadrant 4 is (the most desired state) where security controls were successful in protecting the system or application in question and are fully defended against malicious actors. The simplicity that our two-by-two model offers can be a daily run down of executives and CISO who would ask the managers and the direct reports, “Tell me simply, what is your cyber security posture at this moment.”

**CONCLUSION**

Cyber security challenges are growing every day as computer based technological innovations are expanding at a lightning speed. With every new IT products or an enhancement to existing products, comes the challenges to functional testing on one hand and security testing on other hand. Newer technologies can introduce newer attack surfaces and therefore increase in attack vectors. No organization, therefore, can be entitled to high goal of being “secured”. Unless organizations stay alert and respond to these attacks, the cyber security posture will continue to swing between being compromised to being secured to again being compromised. Our framework is a step towards understanding the cyber security posture as a continuously moving phenomenon.

**REFERENCES**

Ahmad, R., Alsmadi, I., Alhamdani, W., et al. (2023). Zero-day attack detection: A systematic literature review. Artificial Intelligence.

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. IEEE international conference on teaching, assessment, and learning for engineering (TALE) (pp. 62-68).

Alhazmi, O. H., & Malaiya, Y. K. (2008). Application of vulnerability discovery models to major operating systems. IEEE Transactions on Reliability, 57(1), 14–22.

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. Information & Computer Security, 23(1), 102-118.

Ashtari, H., IAST vs. DAST vs. SAST vs. RASP (2024): Key Differences https://www.spiceworks.com/it-security/application-security/articles/iast-dast-sast-rasp-differences

Borges, H., Hora, A., & Valente, M. T. (2016). Understanding the factors that impact the popularity of GitHub repositories. IEEE international conference on software maintenance and evolution (ICSME) (pp. 334-344).

Carley, K. M., Cervone, G., Agarwal, N., & Liu, H. (2018). Social cyber-security. International conference on social computing, behavioral-cultural modeling and prediction and behavior representation in modeling and simulation (pp. 389-394).

Casey, T. (2007). Threat agent library helps identify information security risks. Intel White Paper.

Čisar, P., & Čisar, S. M. (2016). The framework of runtime application self-protection technology. IEEE 17th International Symposium on Computational Intelligence and Informatics (CINTI) (pp. 000081-000086).

Cloud Security Technical Reference Architecture Cybersecurity (2022. https://www.cisa.gov/ sites/default/files/2023-02/cloud\_security\_technical\_reference\_architecture\_2.pdf

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: A review and research framework. European Journal of Information Systems, 26, 605–641.

Cybersecurity, C. I. (2014). Framework for improving critical infrastructure cybersecurity. Framework, 1(11).

DoD Cybersecurity Architecture Division. (2023). Cybersecurity Reference Architecture. https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

Forgerock. (2019). Consumer Data Breach Report 2019: Personally Identifiable Information Targeted in Breaches that Impact Billions of Records. Forgerock Breach Report 2019. San Francisco, CA, USA.

Framework, C. (2021). Getting Started with the NIST. https://www.nist.gov/cyberframework/csf-11-quick-start-guide

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. Computer Fraud & Security.

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior.

Herath, S., Gelman, H., McKee, L., & Dakota State University. (2023). Privacy harm and non-compliance from a legal perspective. Journal of Cybersecurity Education, Research & Practice, 2023(2)

Hinck, G., & Maurer, T. (2019). Persistent enforcement: Criminal charges as a response to nation-state malicious cyber activity. J. Nat'l Sec. L. & Pol'y, 10(2), 271-295.

Hovav, A., & Berger, R. (2009). Tutorial: Identity Management Systems and Secured Access Control. Communications of the Association for Information Systems, 25(Article 42).

Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2(1), 4-27.

International Organization for Standardization. (2020). ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems (https://www.cssia.org/wp-content/uploads/2020/01/ISO\_27001\_Standard.pdf)

Jiang, J., Lo, D., He, J., Xia, X., Kochhar, P. S., & Zhang, L. (2017). Why and how developers fork what from whom in GitHub. Empirical Software Engineering: An International Journal, 22, 547-578.

Juuso, S. (2019). Evaluation of threat modeling methodologies (Master's thesis).Jamk University of Applied Sciences

Karyda, M. and Mitrou, L., (2016) Data Breach Notification: Issues and Challenges for Security Management" (2016). MCIS 2016 Proceedings

Lange, T., & Kettani, H. (2019). On security threats of botnets to cyber systems. In 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 176-183). IEEE.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. International Journal of Information Management, 45, 13- 24.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly, 33(1), 71-90.

Lubua, E. W., & Pretorius, P. D (2019) Cyber-security policy framework and procedural compliance in public organizations. Proceedings of the International Conference on Industrial Engineering and Operations Management Pilsen, Czech Republic, July 23-26.

Malik, M., & Patel, T. (2016). Database security-attacks and control methods. International Journal of Information.

Mann, D. E., & Christey, S. M. (1999). Towards a common enumeration of vulnerabilities. In 2nd Workshop on Research with Security Vulnerability Databases, Purdue University, West Lafayette, Indiana (p. 9).

Marotta, A., & Madnick, S. (2021). Convergence and divergence of regulatory compliance and cybersecurity. Issues in Information Systems, 22(1), 10-50.

Martin, B. (2019). Common Vulnerabilities Enumeration (CVE), Common Weakness Enumeration (CWE), and Common Quality Enumeration (CQE) Attempting to systematically catalog the safety and security challenges for modern, networked, software-intensive systems. ACM SIGAda Ada Letters, 38(2), 9-42.

Microsoft Cybersecurity Reference Architectures MCRA (2023).https://learn.microsoft.com/en-us/security/adoption/mcra

Miller J., (2023). Cyber Compliance 101 – What it is and why it’s needed. https://www.in.gov/cybersecurity /blog/posts/cyber-compliance-101-what-it-is-and-why-its-needed/

Moses, S., & Rowe, D. C. (2016). Physical security and cybersecurity: Reducing risk by enhancing physical security posture through multi-factor authentication and other techniques. Journal for Information Security.

Muckin, M., & Fitch, S. C. (2014). A threat-driven approach to cybersecurity. Lockheed Martin Corporation.

Mughal, A. A. (2018). The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection. International Journal of Intelligent Automation and Computing.

Nasir, A., Akhyari, R., Abdullah Arshah, R., Rashid Ab Hamid, M., & Syahrul Fahmy. (2019). An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications, 44, 12–22.

NISTIR 7622, (2012). Notional Supply Chain Risk Management Practices for Federal Information Systems, U.S. Department of Commerce

Pandya, D., & Patel, N. J. (2016). OWASP top 10 vulnerability analyses in government websites. International Journal of Enterprise Computing and Business Systems, 6(1).

Pascoe, C. E. (2023). Public Draft: The NIST Cybersecurity Framework 2.0.

Pittenger, M. (2016). Open source security analysis: The state of open source security in commercial applications. Technical report. Black Duck Software.

Ponemon Institute. (2020). Cost of Data Breach Study: The US. Sponsored by IBM. Cost of a Data Breach Report. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Portman, R., & Carper, T. (2018). How Equifax Neglected Cybersecurity And Suffered A Devastating Data Breach. In Permanent Subcommittee. United States Senate. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/FINAL%20Equifax%20Report.pdf

Rose, S., Borchert, O., Mitchell, S., Connelly, S., (2020). Zero Trust Architecture, National Institute of Standards and Technology, Advanced Network Technologies Division, Stu2Labs, & Cybersecurity & Infrastructure Security Agency.

Sabillon, R., Cano, J. J., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. International Journal of Computer Networks and Communications Security 9(1), 1-14.

Sallam, R. L., Richardson, J., Hagerty, J., & Hostmann, B. (2011). Magic quadrant for business intelligence platforms. Gartner Group, Stamford, CT.

Scofield, M. (2016). Benefiting from the NIST cybersecurity framework. Information Management, 50(2), 25.

Security of the AWS Infrastructure, AWS, (2024). https://docs.aws.amazon.com/whitepapers/latest /introduction-aws-security/security-of-the-aws-infrastructure.html

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–Information security compliance and violation behaviour in organisations: A systematic review. Social Sciences (Basel), 11(9), 386. https://doi.org/10.3390/socsci11090386

Team, V. R. (2015). 2015 data breach investigations report. Investigations Report. Retrieved from http://www.verizonenterprise.com/DBIR/2015/

Uceda-Vélez, T., & Morana, M. M. (2015). Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Hoboken: John Wiley & Sons, Inc.

Yang, J., Tan, L., Peyton, J., & Duer, K. A. (2019). Towards better utilizing static application security testing. IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP) (pp. 51-60).

Yaqoob, I., Hussain, S. A., & Mamoon, S. (2017). Penetration testing and vulnerability assessment. Journal of Network Communications and Emerging Technologies 2(1), 31-48.

Zhang, X., Yadollahi, M. M., Dadkhah, S., et al. (2022). Data breach: analysis, countermeasures and challenges. Journal of Computer Security.

**ABOUT THE AUTHORS**

**Rashid J Manzar** is a senior member and lead architect in the application and database security department at Verizon. He earned his undergraduate degree from the Indian Institute of Technology, Kharagpur, India. He holds a PhD from the University of Texas at Arlington, an MS in Computer Science and an MBA from the University of Texas at Dallas. He has taught Introduction to MIS, Business Statistics, Data warehouse and Business Intelligence, and Database Management System at the University of Texas at Arlington. He has published in Journal of Database Management and AMCIS. His core technical experience is in the area of RDBMS, VLDB designs, application security, and database security. His research interest lies in Artificial Intelligence, Large Language Models and Generative AI, Penetration Testing, Threat Intelligence, Distributed Design, Security by design, and Application and Database Security. He holds many important certifications such as AWS developer associate, CISSP, CCNA, CCNA Security and Microsoft DBA.

**Rajat Mishra** is an Associate Professor of operations and supply chain management in the department of management and marketing at Stephen F Austin State University. He has published his research in various journals including the International Journal of Production Economics and Operations Management Research. He is a widely cited researcher as evidenced from his Google Scholar data. He is active in the Decision Sciences Institute and Southwest Decision Sciences Institute.