HACx

A Sepio white paper

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

BACKGROUND

The Hardware Access Control Index (HACx) developed by Sepio seeks to assess enterprises' hardware security posture through objective indicators. Typically, hardware security fails to receive the same level of attention and funding as other areas of cybersecurity, such as network and endpoint security, thereby creating a blind spot that leaves enterprises vulnerable. Moreover, malicious actors exploit the visibility challenge by carrying out destructive hardware-based attacks.

The HACx aims to convert this level of vulnerability into numerical values, presenting a clear indication of the enterprise's hardware security posture to improve situational awareness. In addition to an overall hardware security score, the HACx offers detailed risk insights to deliver a more granular assessment. Further, the HACx presents a peer comparison to indicate how the enterprise measures up to its contemporaries which, in doing so, provides context to the HACx scale.

The HACx contains 7 aggregated indicators, comprised of 29 subindicators and 148 microindicators, that look at both the external and internal threat landscape. The HACx relies on primary and secondary data sources to provide an objective assessment of the enterprise's hardware security posture, the results of which get presented on a detailed scorecard.

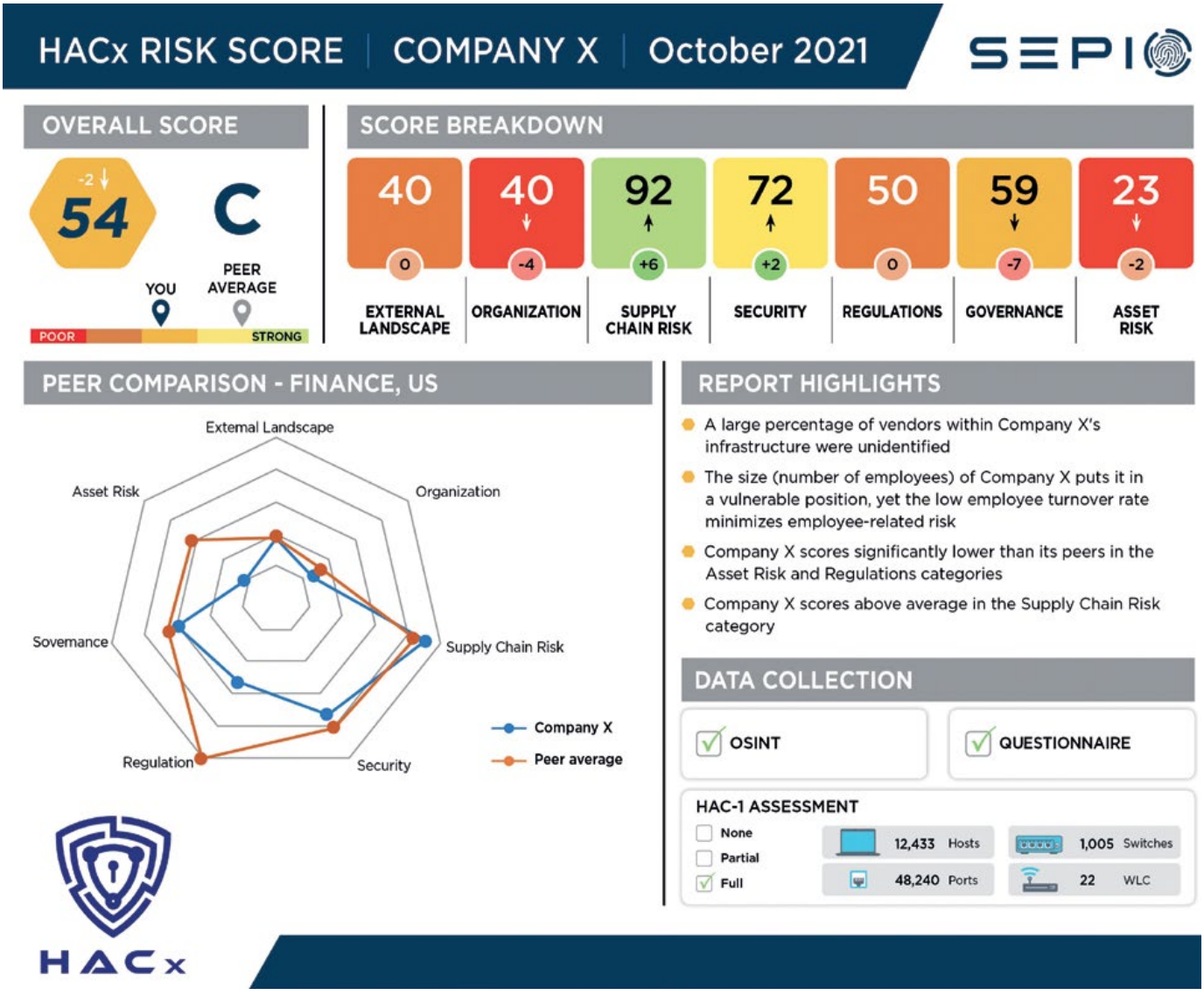
BENEFITS OF HACx

The HACx was created to enhance hardware security awareness and bring clarity to the associated risks. Due to an absence of hardware security solutions available, hardware vulnerabilities go unnoticed, leaving enterprises with the misguided impression that they are less at-risk than they are. Further, because of this blind spot, hardware risks are not factored in when implementing new policies and technologies, leaving a huge gap open on which bad actors to capitalize. The HACx seeks to highlight the importance of hardware security across the entire enterprise.

The HACx guides enterprises to a stronger security posture. Through a comprehensive assessment covering various topics, and complemented by a peer comparison, enterprises improve their situational awareness. With this, the relevant person(s) can make the necessary adjustments to lower the hardware security risk and improve the overall security posture.

As the cyber insurance market grows, the HACx hopes to assist the insurer and the insured. For the latter, the HACx helps lower cyber insurance premiums by providing the necessary insights for enterprises to improve their cybersecurity posture. In doing so, the risk is lowered, thereby reducing the policy cost. For the former, the HACx risk insights offer relevant information for assessing the insured's risk posture. Cyber risk assessments, which are essential to the policy, are often flawed; reports reveal that cyber insurers are concerned that cyber risks are going unidentified. The HACx reveals some of these typically unidentified risks, allowing for a more suitable policy to get generated.

SAMPLE REPORT



SCORING

The enterprise receives an overall score between 10 and 100, where 10 is the lowest hardware security posture (i.e. high risk) and 100 is the highest hardware security posture (i.e. low risk). The score gets complemented by a grade between A and E. Every indicator also receives a score to provide a more granular breakdown.

Further HACx assessments will result in a scorecard that also presents score changes, represented by an arrow going up or down and the numerical value change. This gets applied to the overall score and all indicator scores.

INDICATORS

External Landscape

The External Landscape indicator examines the enterprise's external environment - its industry and geographical location. Such factors are out of the enterprise's control but still have a significant impact on its risk posture. The External Landscape indicator score is not specific to the individual enterprise but rather its sector and territory. As such, the score for External Landscape is pre-defined based on internal research by Sepio's Cyber Research department. External Landscape gets assessed through OSINT.

Organization

The Organization indicator assesses the value and size of the enterprise. The enterprise's value as a target plays a direct role in its risk posture. The size of the enterprise reflects its accessibility which, in turn, influences the hardware risk. Organization gets assessed through a questionnaire.

Supply Chain Risk

The Supply Chain Risk indicator explores the hardware risk posed to the enterprise by its supply chain. Supply Chain Risk also analyses the extent to which the enterprise manages such risk. Supply Chain Risk gets assessed through a questionnaire.

Security

The Security indicator assesses the enterprise's ability to minimize its hardware risk posture through technical and physical controls. Importantly, Security factors in the enterprise's situational awareness to determine the relevance of the implemented controls. Security gets assessed through a questionnaire.

Regulations

The Regulations indicator reviews which (if any) regulations the enterprise complies with. Regulatory compliance lowers the hardware risk due to the enforcement of security requirements. Regulations gets assessed through a questionnaire.

Governance

The Governance indicator assesses the impact that certain policies, practices and processes have on hardware risk. Governance also examines the awareness and prioritization of hardware and cybersecurity risks across the enterprise. Finally, Governance looks at the strategic approach to cybersecurity and how this influences the hardware risk. Governance gets assessed through a questionnaire.

Asset Risk

The Asset Risk indicator examines the enterprise's entire asset infrastructure. Doing so determines the hardware risk level posed by the peripheral and network assets themselves. Asset Risk gets assessed through Sepio's HAC-1 software.

www.srccybersolutions.com +91 120 2320960 sales@srccybersolutions.com

ABOUT SEPIO

Founded in 2016 by cybersecurity industry experts, Sepio's Asset Risk Management (ARM) platform sees, assesses, and mitigates all known and shadow assets at any stage. The only trafficless solution, Sepio is infinitely scalable to protect the company's decentralized, uncontrolled ecosystem as fast and often as anyone, anywhere connects any assets. Sepio provides actionable visibility with the Asset Risk Factor (ARF) score based on a unique Asset DNA generated for each asset at its physical source, reflecting actual business, location, and rules. Sepio Radically improves the efficacy of NACs, EDRs, XDRs & Zero Trust layer solutions that simply see only the assets they are there to protect.
Visit: www.sepiocyber.com

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Highly Automated, and User-Friendly Solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection SEPIO for Asset Risk Management (ARM) to assess and mitigate all known and shadow assets at any scale, THREATX for WAAP (WAF ++) for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS