Cyber Resilience Managed Services

Summary

Security practitioners are increasingly being held to heightened expectations for cyber resilience – that is, the ability to anticipate, withstand, recover and adapt from cyber threats. However, anticipating the many potential threat groups and the hundreds of tactics, techniques and procedures (TTPs) they employ is difficult. Understanding how to withstand attacks across thousands of assets is even harder. Developing a level of confidence that existing business continuity and disaster recovery systems can enable an organization to survive and recover from a disruptive cyber-attack is a challenge for even the largest of organizations, as is keeping pace with adaptive threat behavior.

Through its partnership with High Value Target, The Chertoff Group solves this problem by delivering cyber resilience-related managed services:

- We focus defenses where they matter most. Definitions can be hard, but certain systems are highly targeted by threat actors because they perform functions critical to trust and are thus stepping-stones into everything else. High Value Target's proprietary methodology hones in on often overlooked but critical assets.
- We contingency plan, train and exercise for when things go wrong and increase readiness to adapt against imminent attacks based on a threat-informed approach.
- We develop resiliency reporting that measures performance with transparency, accuracy and precision.

The Chertoff Group Approach

The Chertoff Group develops comprehensive threat-informed defense strategies and operating models that provide direction and repeatability for enabling businesses to implement and sustain cyber resiliency. The Chertoff Group's cyber resilience operating model incorporates these principles through the following elements:

- The Chertoff Group's approach leverages its expertise combined with the MITRE Corporation's ATT&CK framework. ATT&CK is the most comprehensive, authoritative approach to mapping of threat actors to tactics, techniques and procedures (TTPs) openly available today.

- The Chertoff Group's approach is anchored in core cyber resiliency strategic design principles articulated by the U.S. National Institute of Standards & Technology (NIST): focusing on common critical assets; supporting agility and architecting for adaptability; reducing attack surfaces; assuming compromised resources and expecting adversaries to evolve. Taken together, these design principles are intended to reduce the occurrence of threat activity and the potential severity of impacts.

In doing so, The Chertoff Group isolates the following issues and answer these persistent questions:

1. **How do we focus our resiliency efforts?** We work design and implement cybersecurity and resiliency functionality and playbooks for future severe-but-plausible contingencies. We can also develop forward optionality by contingency planning for a tailored set of geopolitical contingency scenarios based on practices used in leading global companies.
2. **How do we know if we are effective?** We practice and validate resiliency processes and technologies to ensure operations as intended while reducing both the likelihood and impact of a severe but plausible cyber scenario.
3. **How do we explain the results?** We develop reporting that conveys cybersecurity and resiliency performance within impact tolerance and risk appetite.

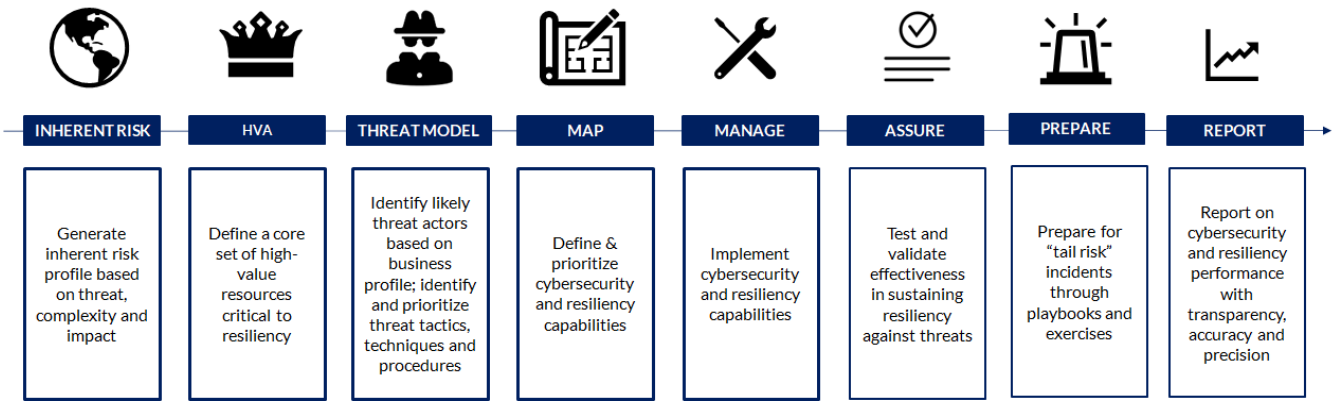
Leveraging High Value Target Know-How to Keep Pace with Adversary Evolution

The High Value Target (HVT) methodology allows practitioners to fine-tune existing business impact assessments and therefore focus on what's most critical: designing and engineering cyber resilience system-of-systems to ensure survivability of essential functions during a coordinated, destructive cyberattack. Developed by highly qualified experts with years of experience managing incident response and crisis events for complex global organizations, we help organizations get the fundamentals right from the very start. We begin with the risk management framework and then build on it with a cyber resilience risk strategy, which is at the core of HVT's service.

Once High Value Targets are identified, secured and continuously validated, an organization's cyber resilience posture is significantly increased.

The Chertoff Group Cyber Resilience Managed Service

The Cyber Resilience Managed Service enables companies to continuously sustain, validate and report on their level of cyber resiliency, as summarized in the following graphic:



Key elements include:

- **Build Inherent Risk Profile.** A strategic design principle for cyber resilience is supporting agility and architecting for adaptability. A starting point for doing so is understanding the inherent risk facing an organization – that is, the risk before mitigations have been put in place – and how that risk is changing, for example based on new business initiatives, mergers & acquisitions or changes in technology architecture. From our experience, three foundational factors define inherent risk: (1) **threat**, (2) **complexity** and (3) **impact**, and we work to build and update business profiles anchored in these elements.

- **Define High Value Assets.** Focusing on common critical assets represents an additional strategic design principle for cyber resiliency. Since most organizations have limited resources to defend the attack surface, it is important to focus defenses on assets that represent heightened risks. Defining "high value assets" can be hard, but certain systems are highly targeted by threat actors because they perform functions critical to trust and are thus stepping-stones into everything else. Such systems do not always rank highly in standard business impact analysis programs. The Chertoff Group and HVT will define and evolve High Value Asset categorizations. Using the HVT methodology, companies can integrate their cyber defense assets and their overall architecture into a MITRE ATT&CK supported, cyber resilience posture with an immediately useful, quantifiable risk method across the cyber terrain.

- **Threat Model.** Cyber resiliency strategic design principles also include assuming compromise and expecting adversaries to evolve. Chertoff Group experts build threat models that enumerate techniques likely to be used by threat actors to achieve initial access, maintain a foothold, and move laterally inside the organization to achieve their nefarious objectives. The Chertoff Group approach is anchored in ATT&CK and tailors the weights for each threat object. The threat model is regularly updated based on changes both in the business profile and threat actor capabilities and intent.

- **Map & Manage.** An understanding of threat is academic unless it can be practically applied by ensuring measures are in place to address such threats. The ATT&CK framework and NIST resiliency guidance include mappings of threat techniques to mitigations and data sources, and The Chertoff Group team helps ensure that these defensive measures are practically applied across a client's environment.

  A related strategic design principle for cyber resiliency is reducing the attack surface, which reduces the likelihood of incident occurrence and related impacts. The Chertoff Group ensures defenses are applied across the attack surface in a risk-informed manner.

- **Assure.** Adversary emulation testing not only validates that controls are operating as intended, but also supports the strategic design principle of expecting adversaries to evolve. The Chertoff Group identifies critical threat techniques, including updates as threat profiles change, and prioritizes them for periodic adversary emulation testing, providing clients with the assurance that key defensive capabilities are operating as expected.

- **Prepare for Incidents.** In a world where there is no such thing as risk elimination, incident preparedness is critical to minimizing impact from a successful intrusion. Preparedness supports the strategic design principle of agility and adaptability and mitigates organizational brittleness that could cause catastrophic consequences in an incident. The Chertoff Group works with clients to develop plans, playbooks and exercises critical to sustaining a baseline of good practice and muscle memory on how to respond to high-severity incidents. This includes accounting for loss of integrity and confidentiality within traditional restore and recovery plans, which calls for not only secondary but even tertiary arrangements to deal with plausible adversity.

- **Report.** We also help organizations report on cybersecurity and resiliency performance with transparency, accuracy and precision. *Transparency* comes from using authoritative security frameworks from places like the U.S. National Institute of Standards and Technology (NIST) and the MITRE Corporation that are repeatable and auditable. *Accuracy* marries these frameworks with a detailed analysis of likely threat techniques to ensure that resiliency measures map to these threats and are operating as intended. *Precision* evaluates whether the first two steps are applied in a manner that is appropriate to the type and riskiness of relevant assets.

About The Chertoff Group

The Chertoff Group is an advisory firm of highly qualified experts that uses proven frameworks to help organizations achieve their business and security objectives in a complex risk environment. Our team helps organizations manage cyber, physical and geopolitical risks; navigate evolving regulatory and compliance requirements; and discover opportunities to win business and create value. Through our investment banking subsidiary Chertoff Capital, the firm provides M&A advisory services to companies in the defense technology, national security and cybersecurity markets. Together, we enable a more secure world. For more information, visit www.chertoffgroup.com.

About High Value Target

High Value Target is a boutique cybersecurity research firm that specializes in designing methodologies aimed at significantly increasing an organization's cyber resilience posture against sophisticated cyber threats. We are actively engaged in leading cybersecurity communities and collaborating with best-in-class peers such as MITRE, ISSA, FIRST, NIST, OASIS Open. For more information visit www.highvaluetarget.org.