EITS
Enterprise IT Security

Security Assessment

We hear you.

5 Most Common Reasons Customers Consider an EITS Security Assessment

- "We don't have time - our team is slammed managing day-to-day tasks, not to mention the ever-growing project list."
- "We have an upcoming audit, a security assessment will help us prepare."
- "Merger / acquisition conversations are taking place, this will better enable the business to quantify cyber risk."
- "I am a new CISO (or CIO) who wants to fully understand and quantify our cyber risk."
- "We are building our security team and have knowledge gaps; we need experts we can trust to give us an outsider's agnostic opinion."

It all boils down to RISK Management

At a high level, security assessments are about identifying, prioritizing, and managing risk for your organization. This boils down to understanding your current security controls, supporting processes, and potential areas for improvement. Data results are used to enable the right security investments on a go-forward basis.

Although a framework and standards are key in this process, we believe each customer requires a tailored fit based on taking into account their priorities and where they are in the Cyber Security Maturity Model. EITS puts a heavy focus on sizing up the right tailor fit for each customer statement of work to ensure expectations are communicated, understood, and exceeded.

Leveraging the right assessor / technical resource is critical to a successful security assessment. EITS aligns our assessors based on experience in industries and/or specific compliance requirements customers may have; for example, the needs of manufacturing customers can greatly differ from those of healthcare or financial organizations. Our team brings a combination of experience identifying and quantifying risk in addition to managing risk and solving security challenges from a customer's perspective.

Though we utilize a three-step assessment process (identify, prioritize, and manage), each step is structured and methodical. Please see the second page for more information regarding our process.

Our Process

Identify

If you cannot identify the target - you are the target! Start by understanding likely adversaries and their capabilities. Using the NIST CSF (Cybersecurity framework) as a foundation, we develop an understanding of risk to systems, people, assets, and data.

- **Inventory** - Physical and software assets to establish a foundation for asset management
- **Assess Business** - Identification of business environment(s), role(s) in supply chain, and critical infrastructure
- **Policy** - Identify existing or required policies to define governance program, legal and regulatory requirements, and potential cyber security gaps
- **Vulnerabilities** - Exposures to internal / external resources that can be exploited by an adversary; risk response activities are also a basis for risk assessment
  - This goes beyond vulnerabilities on internal physical or software assets and into identification of potential flaws in a customer's existing security controls / architecture

Prioritize

More often than not, organizations will be faced with cyber risks far beyond what can be solved in weeks, months, or even years. "Leaders aren't just paid to make decisions on what to do; it's just as important for them to make decisions on what not to do," said Naveen Zutshi, Chief Information Officer at Palo Alto Networks. The ability to prioritize what can realistically be done, and push lower priorities out, is critical to a successful security program.

An example of outcomes includes:

- Stakeholder matrix
- Gap analysis / roadmap
- Threat inventory
  - Categorize
  - Probability scale
  - Impact assessment
  - Financial impact
- Security Criticality Rating– A structured way to assess the security criticality of software and supporting physical infrastructure based on the sensitivity of data and criticality to the business
  - "Start with the crown jewels–data on your employees and your customers," said Zutshi. "If those are compromised, you may not be able to recover as an organization."

Manage

Using a risk management strategy, we work with customers to establish risk tolerance and a risk register process, which are then used to prioritize and manage risks.

- **Supply Chain Risk Management Strategy**
  - Priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated