

Business Threat Modeling



Business Threat Modeling^(TM) is an innovative way for a business unit to diagnose and quantify threats to the operation: threats of fraud and data loss:

- Delivered as a consulting study on a fixed-cost basis, with deliverables in 2 work-weeks.
- Executed by highly experienced consultants with specific experience in global organizations.
- Diagnoses threats to IP and customers
- Analyzes value at risk in financial terms
- Produces a plan for prioritized, cost-effective security controls

Event risk is not your only operating risk

Historical risk data is not sufficient to predict the next threat to your business given how interconnected and how fast the world is moving today. Instead, a substantial amount of operational risk may come from business threats that are **not** predictable by traditional risk modeling. Modern networked organizations are vulnerable to unpredictable, high-impact fraud and data loss and are exposed to huge losses beyond what traditional risk models project. These events have three characteristics:

1. Appear as a complete surprise to the institution.
2. Result from links and interdependencies outside the enterprise.
3. Are 'explained' by human hindsight, after the fact.

Making better decisions

We challenge the assumption that it makes sense to allocate capital against the likelihood of fraud and data loss on the basis of technology features. In order to decide *what* security countermeasures are best - we diagnose threats and their potential impact by testing two key hypotheses:

1. Hypothesis # 1: Data loss / fraud is currently happening in the business unit, at a level justifying a capital investment
2. Hypothesis # 2: A cost-effective set of robust security countermeasures exist that can reduce risk to acceptable levels.

How does Business threat modeling work?

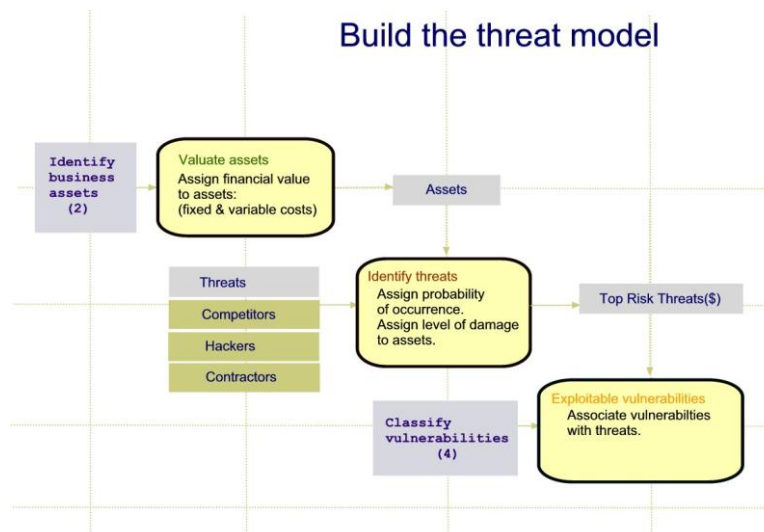
Human requirements

A Business threat modeling study is sponsored by a senior manager such as CFO or COO. Typically, 3-7 representatives from the business unit in operations, finance, marketing, security, IT and risk management participate in the study.

- **1 week before:** Planning meeting with consultant and sponsor. Decide on the scope of business assets and activities to be studied. Brain-storm hypotheses and sub-hypotheses to be tested in the study
- **Day 1:** Start automated data collection with network surveillance.
- **Days 1-2:** Build the threat model with focus group. Collect data on vulnerabilities, threats and assets from the group and from the network surveillance. Test the study hypotheses. Quantify value of assets.
- **Day 3:** Sponsor and analyst present findings to management
- **1 week after:** Present final written report to sponsor

The data collection and risk analysis process

Data is collected from the network using passive network surveillance. The interview process performed by the consultant with the study group is facilitated with a wall-charting technique. Originally called RAMS (Requirements Analysis of Manufacturing Systems); the method was developed by Kari Saaren- Seppala from Finland. The approach improves communications across organizational boundaries, resulting in greater management involvement and a clearer understanding of specific business and security requirements.



The PTA (Practical Threat Analysis) software is used to automate the risk calculation process and store data collected from the group and from the network surveillance in a database. Analysts and stakeholders can quickly create new threat scenarios and analyze financial impact.

Technical requirements

1. A conference room for 4-5 wall charting sessions with the group for 2 days.
2. The Control Policy Group will provide a passive network surveillance device to detect security violations by observing network traffic.

Deliverables

Findings will presented by the sponsor and analyst at the wrap-up meeting:

1. Did we prove or disprove our hypotheses regarding fraud/data loss events?
 - What are the data types and volumes of data leaving the network?
 - Who is exploiting vulnerabilities to manipulate or steal data?
 - Where is the data stored?
 - Where is the data going?
 - What are the current violations of company Internet Accepted Usage Policy?
2. What security controls are needed to support the information behavior you want - sensitive assets stay inside, public assets flow freely, controlled assets flow quickly?
 - What are the top risk threats?
 - What is the value of information assets?
 - What is the value at risk from each threat?
 - What is the cost of the security controls?

