All.Net Analyst Report and Newsletter

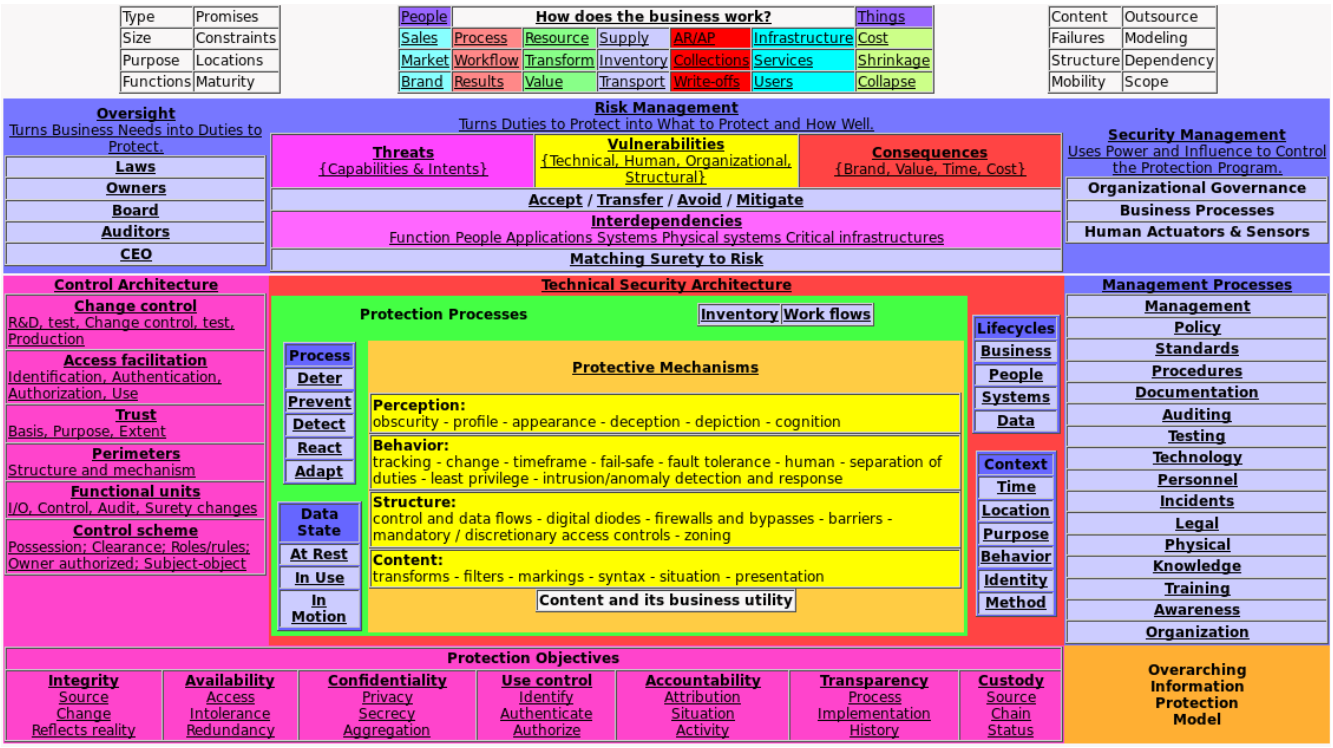
Welcome to our Analyst Report and Newsletter

The cyber security brain

Every successful human systems activity ultimately ends up operating like a cognitive system. That is to say, the system uses the cognitive properties of the components to form a cognitive system of the composite.[1] These cognitive systems are – by definition – cybernetic. They have sensors, actuators, communications, and decision-making mechanisms integrated into a system, usually in complex connected patterns.

Cyber security as a "cognitive system" (brain)

Of course cyber security is a brain within the brain of the enterprise it operates within. As such, compatibility of the overarching enterprise composite with the cyber security components, is vital to the success of cyber-security. One approach to understanding how to do this in context is the approach of the diagram shown here:



The overarching structure of the brain is that it starts with the composite and its operational requirements (How does the business work?). Based on these results, and taking into account the ways the composite can fail if components fail, oversight then defines the duties to protect. Risk management priorities duties and security management operates the cognitive system that uses (human and automated) actuators and sensors. These human and automated mechanisms than apply decisions to meet protection objectives structured via control architecture to control protective mechanisms which execute in the digital realm.

1 The mental action or process of acquiring knowledge and understanding through thought, experience, and the senses. (https://en.oxforddictionaries.com/definition/cognition)

Embedded cognitive systems

Thus the cyber security composite is an embedding of the business concept.

- The operational needs of the business drive the overall enterprise brain:
  - The oversight brain involves people with different roles and responsibilities who form up a set of duties to protect, normally over a long time frame, adapted to meet the changing needs of the entity and its operating environments.
    - The risk management brain involves people who take the duty to protect into account along with other balancing concerns in order to make decisions at a shorter time frame about what management decision frameworks to put in place and how to support day-to-day decision-making.
      - The protection management brain is typically headed by the Chief Information Security Officer or someone with a similar title who influences people to generate desired behaviors and observes results using metrics combining human and automated sources. Communication is via meetings and media.
        - The control architecture is used to structure and operate the execution brains. This architecture is a meta-level entity that identifies the organizational principals of how things operate.
          - Multiple execution brains operate together and at different levels to ultimately control the mechanisms to meet operational needs.

Properties

Each level is involved in decision-making with different properties associated with decisions. These properties include the types of decisions, time frames to make the decisions, involvement of individuals and/or groups, different levels of expertise and preparation, etc.

- The oversight brain typically operates in time frames of months to years, often reflecting changes in the business and how it operates. These decisions tend to be subjective, qualitative, ordinal or nominal, complex, predictive, group, formal, textual, strategic, satisficing, architectural, high expertise, static, and with multiple intentions.
- The risk management brain typically operates at time frames of weeks to months and often quarterly or annual reviews are used for major decisions. These decisions tend to be objective, quantitative, interval or ratio, simple, predictive, individual, formal, strategic, optimizing, model-driven, amplitudinal, designed, high expertise, static, and with single intentions.
- The protection management brain normally operates at cycle times from 1-week to 1-month and often has quarterly and annual decisions with multi-year planning on occasion. However, in situations where high consequence incidents are underway, escalation may occur to where the CISO makes decisions on a minute-to-minute basis with decision times on the order of seconds to minutes. Decisions tend to be subjective, qualitative, nominal or ordinal, flat, simple, explanatory, individual, casual, tactical, satisficing or incremental, data and knowledge driven, amplitude and architectural, ad-hoc, high expertise, dynamic, and with single intentions.

- The control architecture identifies decision frameworks implemented in different time frames, typically ranging from minutes to far shorter times. Decisions tend to be subjective, qualitative, nominal, simple, predictive, group, formal, strategic, optimizing, data, model, knowledge, and user-driven, architectural, ad-hoc, high expertise, static, and with single intentions.
- Execution brains make decisions in time frames ranging from real-time (less then a millisecond) to seconds, with human interaction schemes often taking seconds to make decisions. For lower priority items, time frames may be minutes or more. These decisions are almost always objective, quantitative, interval or ratio, simple, explanatory, individual, formal, textual, tactical, cybernetic or satisficing, driven by communications, data, and/or users, amplitudinal, programmed, medium- to low-expertise, dynamic, and competitive.

Complexities of the differing brains

Part and parcel of the multitude of brains involved in cyber-security operations is the fact that these various different sorts of decision-making system operate at different tempo and with different motivations and criteria. There is an old saying:

The army is designed by geniuses to be executed by idiots.

Of course this is no longer true. To even use many modern weapons systems, you need a combination of education and training. To use them well or adapt in the field, requires quite a bit more.

Technical cyber security systems today tend to be designed by hackers to be operated by hackers. In order to manage the hackers, the corporate governance has to be aligned to their behavioral patterns and designed to effectively influence and observe the people and systems in the context of the situation. This in turn has to both operate in the context of the overall composite and co-operate with the CISO function, within the parameters of risk management, based on the defined duties, and be integrated and operated at the top level by the CEO.

Fusing these diverse brains into a cohesive cyber-security brain is not a simple matter. Protection has to integrate into the overarching business operational methodology in order to be functional and effective. This ultimately comes down to the integration of a very large set of decisions, well beyond what can currently be planned or analyzed. Given the different nature and their time frames, care has to be taken regarding focus of attention, thrashing, confusion, deployment, and other aspects of change and timing.

Conclusions

The best way we have found to do this fusion today is by identifying a set of about 100 architectural decisions that set overarching strategy and tactics for the enterprise. This includes time frames and responsibility for decisions, roles and responsibilities, matching surety to risk, power and influence associated with decision-makers, and so forth. These decisions are tied to the context of the enterprise using standards of practice that have been tested and applied across many enterprises and are then customized to the entity by experts working with top management. Proper invocation requires ongoing collaboration between those in charge of the decision-processes and experts in the relevant fields working together on a regular basis. So that’s how you create and operate an enterprise cyber-security brain.

