Cyber Entropy, A Theory of Cybersecurity

The theory of cybersecurity is:

I'm thinking,

Unfortunately, there isn't one – yet.

Just take a look at marketing, a body of literature that's over a century old, and still no accepted theory. There are many models; you may have heard of the 4P's, Price, Promotion, Product, Placement. Channel Marketing, Porter's Five Forces, a Strength, Weaknesses, Opportunities, and Threats (SWOT) analysis, the Balanced Scorecard, the Marketing Mix, I've even seen Maslow's Hierarchy of Needs used a marketing theory. However, there is no accepted universal wide marketing of theory. Even Information Technology's body of literature, some of which started back in the '40s has no universal wide accepted theory.

That now brings us to the world of cybersecurity. When did this body of knowledge begin?

It is hard to pinpoint since we do not even use a common name, e.g., is it the theory of security, the theory of information security, the theory of information assurance, operations security, network security, it is hard to come up with a theory when we don't even use the same language. So, it's not surprising there isn't a theory.

There are many models we use in security research, e.g., ISO, NIST, DHS, NSA, IEEE. Also, many theories such as Game Theory, Adoption, Neutralization, Warfare theory, etc., have also been used in security research, so perhaps we can start there.

To formulate a cybersecurity theory, we need to have a foundation for theory, and Gregor's (2006) model of theory is a good place to start, and we expand on that with Horne, Ahmad and Maynard's (2016) framework of the information technology discipline.

5) Finally, in design we have more than enough models, Protection Motivation or the Unified Theory of Acceptance and use of Technology models and apply cybersecurity concepts. We can adapt and replace the constructs most likely aligned within a cybersecurity focus.

Therefore, by starting with Gregor's (2006) explanation of theory development, and examining current theories used in cybersecurity research, we might come up with a cybersecurity theory to discuss.

In all of these areas, they all point to one thing, and that is data or more appropriately information.

Cybersecurity is protecting information, anywhere, anytime, even a person in the general sense is information for what they know. That is why when we calculate risk, we do not look at the value of data, but the time value of information.

Companies spend millions of dollars protecting their chief executives rather than an employee. Nations spend millions protecting their Presidents than average civilians, so what are they protecting? The person, or the information the person has, therefore, even a person can be summed up in a common denominator along with technology in that it's the information we are protecting and not just the information, but the cyber entropy of that information.

Since we now have several parts for a model of the theory of cybersecurity, we also need independent and dependent measures. Since entropy is a condition of the unpredictability of the state, and in this case information, we could set this as a continuous dependent variable. The rate of loss of information is dependent on its entropy, that is how effectively the information is protected. Then borrowing from Gregor's (2006) work, the other areas are cause for that information entropy, could be dependent clauses. Looking at a model of cybersecurity, we could imagine the following.

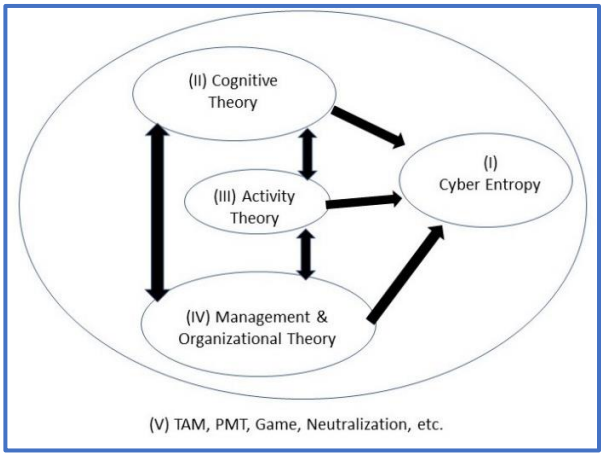
This adapted model of theory would encompass five areas, 1) analysis, what is the phenomena we are trying to explain, 2) can we explain the phenomena, 3) can we predict the future looking, 4) prescription, what will happen given change, and 5) design a model, a technique, some way a relationship can be tested.

Building upon these, we can construct a model of cybersecurity.

1) In analyzing, the phenomena under consideration; it is the loss of information, i.e., the loss of system resources, the loss of personnel, loss of information is the core component, or Information entropy, the greater the entropy, the greater the chance of loss of information. Information entropy is a concept from information theory and is the amount of uncertainty in information. In our view it is the amount of uncertainty safeguarding that information, perhaps we could term it cyber entropy to differentiate from information entropy in that the term looks at entropy from the cyber perspective as the general term entropy is used a lot in different disciplines.

2) In explanation, we want to explain the entropy of the information, not just why we lose the information, but why the cyber entropy of information increases. Are hackers breaking into computer systems, are companies not using secure hashes when storing data? Successful Social Engineering attacks. These are human behavioral traits we should seek to address. Even technology issues are often traced back to an underlying human issue. Could Distributed Cognitive Theory help to explain here, cognitive experiences and differences help to explain a person's motives, so perhaps this will help to explain cyber behavior.

3) In prediction, are we looking at future behavior of the phenomena? Will we be able to predict the future cyber entropy of information, i.e., from the number of factors present, can we measure with any reliability future entropy measures,



Cyber Entropy, A Theory of Cybersecurity

In this theory of cybersecurity, the entropy of information "Cyber entropy" is dependent on multiple factors, which taken together will impact the increase or decrease of entropy of that information. As the entropy increases, the more chance that the information will become compromised.

As various factors motivate our security behavior, the more we understand these factors, the more we can take better protection measures, which will lower the entropy, and the safer the information will become.

Here, the factors that impact our (II Cognitive Abilities), (III Social Activities Behaviors), and (IV Management and Organizational Cultural factors) could help shed light on the cyber entropy of information within our organization.

The model is adapted within the context of the various information systems models we have now, that is, for example, within (II Cognitive theory), we would want to examine constructs from the relevant literature like Game theory, Adoption, Neutralization. In (III Activity theory), we might examine constructs from the social engineering literature.

correlation, causation, regression, etc. Perhaps we could borrow from Activity Theory that helps to explain how humans seek to accomplish tasks with resources, in this case, technology. 4) Can we build a prediction model that will help us to show the relationship to information loss? We could borrow from management and organizational theories to build hypotheses to test the theory. The psychology of blame and increased stress levels attributed to cybersecurity professionals, arising from pressure from management and organization culture could contribute to behavior.	This model emphasizes the human behavior more closely than other models but is grounded in the literature about cybersecurity and other technology-based literature. Gregor, S. (2006). The Nature of Theory in Information Systems. MIS Quarterly. 30. 611-642. 10.2307/25148742. Horne, Craig & Ahmad, Atif & Maynard, Sean. (2016). A Theory on Information Security. The 27th Australasian Conference on Information Systems, At Wollongong, Australia