All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Cyber Security Intelligence

For a long time, the intelligence and counter-intelligence aspects of cyber security have been considered a lesser element among many in the field. When people I know bring up things like perception management and counter-influence they are often told that’s not part of cyber security.

My view of this is pretty simple. If people are using something to defeat protection, it is part of the field. Put another way, anything that reduces the assurance of information or related technology having the desired utility, it;s a cyber-security problem.

Fundamentals

My viewpoint stems from a fundamental approach I have long held that information protection, which has evolved into cyber-security, is about assuring the utility of content. Increasingly, as information (syntactic and semantic content) and information systems have moved into the cyber (sensors, actuators, communications, and control) arena, the utility of content has moved into the utility of systems as a whole. That is because of the now more direct interaction between cybernetic technology and the details of day-to-day life.

Of course utility is a function of viewpoint. Russia’s utility lies in disrupting global democratic societies and breaking up the Western alliance. The West’s utility lies in supporting those same institutions. So protection for the West is about assuring some view of truth, openness, and honesty, while protection from the West for Russia is about assuring a lack of group, national, and global cohesion of the Western countries and alliances.

A sense of what has changed

This is nothing new. Intelligence operations of nation states have created and applied these methods for a long time. Corporate espionage has been an under emphasized component of most programs for many years. It’s hard to think about your competitors as illegally acting against you unless you have experienced it. Of course in select industries, this has long been understood, but in most companies, especially smaller ones, there has been little apparent threat, and more specifically, they would not know if they were being exploited till too late.

The automation and access brought on by the Internet has increasingly led to attacks against enterprises in the $1M/y revenue level. Thefts of tens of thousands to hundreds of thousands of dollars are increasingly used by more sophisticated actors who have realized that:

- Attacks on smaller companies are unlikely to be detected quickly (or at all).
- Automatic or nearly automatic theft of $10K a thousand times is $10M, why not?
- The response to a $10K theft by law enforcement is likely to be limited or less
- The ease and cost of such attacks is very low.

Easy, low cost, low risk, automatic. Better, cheaper, faster crime. Wouldn’t you?

But of course once tested in the small, why not go for the bigger targets? And so they do.

Broken windows

Cities have found that if you leave buildings with broken windows, their neighborhoods become more crime ridden. Indeed the more you ignore small crimes, the more larger crimes you tend to get. That's what happened in the cyber arena. Cyber-security folks have been issuing warnings, demonstrating realities, and complaining about top management ignorance for as long as I can remember… and I am getting pretty old!

Once the veneer of being unassailable departs, the dogs of war start taking their bites. Before long, you find yourself eaten by packs of wolves, struggling to survive.

The West has shown its weakness, enterprises have taken bigger risks for bigger rewards, and those risks and understood weaknesses have produced the wolf packs of threat actors.

Over time, as the wolves have succeeded, the ants come marching in after them. We have created a society where slander is commonplace, where lying for advantage is increasingly accepted, where "truth" is relative, and where "alternative facts" are treated as ground truth.

We reap what we sow.

I heard the expression "less is more" and I scorned it as "perception is reality". Less is not more. It's less. The expression, as meaningful as it may be in terms of identifying that finding more efficient ways to do things (less) produces better outcomes (more), is problematic in our society, because it has gone beyond the expression of a concept and become the asserted reality in itself. The expression replaced the concepts, but then the words of the expression replaced the expression, and some people now believe that lies are truth.

So now we need to find a way to counter the very problems we have created and ignored. Some are **not** more equal than others, reality **doesn't** care about what you perceive, and less is **not** more. You should try to **do more with less**, **perceive reality**, and "***I don't say I'm no better than anybody else, but I'll be dainged I ain't just as good***" (*Oklahoma*).

Come intelligence

I have recently added (and continue to add) Intelligence to the Standards of Practice. In particular, I have identified coverage of:

- External, Inbound, Internal, and Outbound
    - **External**: Not directly touching the defender enterprise
    - **Inbound**: Coming from outside toward the enterprise
    - **Internal**: From and to within the enterprise
    - **Outbound**: From the enterprise to the outside
- Intelligence, Influence, Threat, and Sharing
    - **Intelligence (and counter-)**: Seeking (and denying) reliable authentic information
    - **Influence**: Affecting decisions and actions through information
    - **Threat**: Actors with capabilities and intents affecting the enterprise
    - **Sharing**: Getting/giving information from/to collaborators for mutual benefit

Regardless of how it is done, enterprises must face these issues.

Placement

The question, as usual, is not whether to address these items, but rather how and where and by whom they should be addressed.

Obviously, they have effects across a wide spectrum of the protection program and the enterprise as a whole. But as all such things, they must be managed somehow. For this reason, I have placed the explicit management of these items within the purview of the security management process in the standards of practice.

Of course there are other interactions across the spectrum. From the business drivers that identify the consequences of failures of protection in these arenas to the defined duties to protect, through risk management, and into the operational management. And under the management control are the effect in protection objectives, control architectures, process, lifecycles, context, inventory, work flows, and protective mechanisms.

But at the core, there is a management process that must identify the basis for undertaking (or not) countermeasures, and what those countermeasures are for specific aspects of specific enterprises.

Some idea of the implications

We are still working through the details, and we welcome your ideas and assistance. Here are some starting points:

- **Public relations**: PR campaigns run by the marketing department have traditionally been the home for carrying out responses to threats to brand. But PR departments are not well prepared for viral spread of rumors and counter-messaging. How will cyber-security interact with marketing to mitigate the effects of such threats?
- **Operations Security**: How does the operations security program deal with external intelligence operations without adversely effecting normal use and operations?
- **Deception operations**: The threats are using large-scale global deception campaigns. How do we apply deception and counter-deception techniques, technologies, and vendors effectively to counter their campaigns?
- **Control placement**: The introduction of new technologies, vendor types, and activities implies the need to update the overall control scheme. What do we do where and in what way to change the controls?

The list goes on and on, of course, but this should give you a sense of the challenges enterprises face in this arena, bit in terms of some of the specifics and the larger picture of how this effects the overall cyber-security program.

Conclusions

It’s time we made explicit the intelligence operations aspects of cyber-security. While always an inherent embedded function, the increased use of previously **state tradecraft deployed by** and for them and **an increasing array of other threat actors** against more and more targets, almost certainly **including your enterprise** if you are of substantial size, implies a need to act, both generally as a field and specifically as an entity.

Build your cyber-security intelligence program