OPINION

THE TRAP OF INFORMATION SECURITY" & ESCALATING CYBER RISK

JACK WHITSITT
Jack Whitsitt is a senior strategist at EnergySec. During his 14 years activity in both Information and Cybersecurity worlds he has written open source honeypot tools and operationalised security data visualisation theories. He had national control system incident response responsibilities, led large scale public/private risk management initiatives on behalf of the government, occasionally giving advice on international policy matters. He also teaches his own class at EnergySec on using frameworks to bridge the business/technology risk divide.

In the modern world we have come to accept that cybersecurity concerns are a fact of life. Whether we are wearing the filters of a seasoned general, a government leader, a software engineer or just a regular person, we know that cybersecurity matters to us. This has resulted in the development of a massive "Information Security" industry, new laws and policies, changes in insurance industries, and even Hollywood film and TV series. But has this progress been helpful? Of course any progress that moves the state of the world forward must have some positive elements. But will it get us to where we want to be? Likely not.

This is because, presently, "Information Security" is helping to perpetuate and escalate cyberconflict, not reduce it.

How can this be? Information Security, after all, gives us more weapons with which to defend ourselves and almost every conversation in almost every cybersecurity forum revolves around creating better defenders and tools: Bastion defence positions, arms, intelligence, logistics of responses, attribution, etc. are all at the forefront of cybersecurity thinking.

There appears to be in this thinking, though, an assumption of long-term sustained conflict. Little thought, if any, seems to be given to sustained reduction of exposed surface area, enabling rapid risk pivoting in socio-political institutions or partnerships, or what a (cyber) secure world would even look like.

What would it look like? It's actually hard to discuss in terms of "Information Security" because, as a pseudo-discipline, it presents strategists with several framing problems that must be examined to understand the nature of cybersecurity risk and how it can be reduced – and the appropriate model to use is not necessarily obvious. We've been getting it wrong for a long time.

For instance, the idea of networks or perimeters being "broken into" by "hackers" is no longer a helpful framework for understanding cybersecurity. Instead, strategists should consider cyber risk to be a parasitic problem space. In this space, entities compete for the use of common systems to produce value – some of them legally, others not.

> "There are no individual networks or infrastructures any longer.

It is helpful here to understand that there are no individual networks or infrastructures any longer. If an entity "purchases" or "builds" a "system," what they are really doing is adding components to a single internet; they are not building their own "networks." These entities might then have the "legal" authority to use their section of the internet to produce value, but it is not a separate system.

When subsequently examining what "risk" and

"hacking" and "cybersecurity" look like on this modern, shared internet, it should be clear that our "adversaries" resemble parasites attempting to hijack our collective infrastructure in order to attain their own ends. These ends might include halting the legitimate value being produced, altering it or generating entirely new outputs. In all cases, however, there is a sustained competition between all parties for value production. Further, the only difference between legitimate entities and "adversaries" is a matter of legal perspective and faith in ownership of systems that are not really separate from each other.

> "The idea of individual incidents being the focus of security efforts is less than helpful.

This situation has several implications for managing security.

1. The idea of individual incidents being the focus of security efforts is less than helpful. The internet exists in a constant state of compromise, conflict and risk. There may be individual "infestations" of a subsection of the internet, but those are often tangential to the overall health of the underlying system. An excessive focus on managing these infestations can hinder a more useful focus on the management of factors affecting the entire system.

2. Security cannot be achieved by independent entities alone. It is simply not possible. There are massively matrixed supply and trust interdependencies involved in every aspect of the internet. When managing a parasitic problem, the collective components of a system must work together to reduce the exposure area so that the likelihood and associated costs of actual infestations are manageable over time. Without collaboration and co-operation across "legal sub-component" boundaries of our infrastructure which are the most fundamental requirements, the surface area needing management by individual entities will continue to increase with every line of code written, every additional connection made and every new user – but without the benefit of economies of scale and shared resources applied to the collective problem sources.

3. "Adversaries" hold several high points as opposed to "legitimate" system owners. Adversaries are not always bound by the same "soft" constraints as others (i.e. law); they are able to utilise and exploit single exposure opportunities over time without being required to hold a constant line (thereby allowing more flexible resource utilisation), and have (whether in league with each other or not) collective impact on the resources and environmental stability of "sub-internet system owners" who are often prevented from collaborating by political, legal, and cultural barriers.

4. When cybersecurity is looked at as a value-production competition in a parasitic environment, it should be very clear that the goal of cybersecurity is not "security." In fact, there is no such thing as "cybersecurity" as a strategic goal. Instead, "cyber" goals are intrinsically and unavoidably tied to our existing value production goals. This means that any efforts to improve security sustainably that do not include value production mechanisms in their scope are doomed to fail.

> "Any efforts to improve security sustainably that do not include value production mechanisms in their scope are doomed to fail.

5. Most importantly, cybersecurity is a human-driven state that encompasses both human and

technical systems. There are no security states that are not created by an aggregate series of authorised decisions by people in authorised roles somewhere on a timeline. Humans are the sole causal factor in our cybersecurity risk and any attempt to reduce risk that does not acknowledge improving decision-making capacity as a primary goal is doomed to fail.

Taken together, these factors and perspectives demonstrate that our model of information security is severely broken. Entities are not – as most information security practices assume – individual defenders who can, with sufficient resources, willpower and effort, hold bad actors at bay indefinitely in a way that maintains their desired level of "security."

Instead, we are all under siege in a hostile environment by opposition that holds high ground and is difficult to dislodge. This is an important point. Few, if any, individual entities on the internet have or will ever have the visibility or ability to make effective risk based decisions. The scope of their influence, ownership and resources – whether industry, government, or citizen – is simply not broad enough to manage all of the variables involved in breaking a siege. Left in isolation, entities are forced to do the best they can in the fact of the escalating costs associated with increasing complexity against a broad mix of adversaries who face massively different constraints which are, broadly and asymmetrically, in the adversaries' favour.

Unfortunately for everyone, "information security common practices" are not effective at coping with any of this. These are common practices as we know them today:

1. Treat companies as defenders and so create a continuous mismatch between expectation and capability. Attempting to enable a company's ability to fight off a single attack might make sense. But that's not what is happening. Instead, those attacks (and, importantly, the simple possibility of those attacks) are putting funded, thoughtful, sustained, direct and indirect pressure on organisations. This requires different kind of resource commitments and capability competencies. Few, if any, organisations are able to sustain them.

2. Require trust boundaries that assume a securable perimeter of control (if not a network perimeter) that poorly reflects the reality of operating in modern society. Attempting to apply secure authentication, authorisation, encryption, monitoring, code verification, etc. across every actual relevant trust boundary rapidly looks hopelessly tangled. This has the effect of isolating control authorities who should be collaborating into false perimeters and creating a resource black hole which can never be sufficiently filled with information security controls.

3. Focuses on managing individual (real or potential) incidents as opposed to removing the sources of systemic exposure introduction and instability. This obscures visibility into environmental risk and does not assure generally defensible organisational behaviour. Organisations can implement the world's most effective incident management controls and yet still introduce enough exposure outside the scope of "Information Security" controls to overwhelm their own capabilities.

4. Create situational awareness disconnects between stakeholder needs, actual exposure, and provided data. The NERC CIP regulations in the U.S, for example, are designed with no threat model in mind and, while they may or may not have an impact on the ability of adversaries to intrude into "networks" (as measured at single points in time), the regulations do nothing to provide government officials with knowledge of their

infrastructure's exposure to cyber risk or its overall defensibility against thoughtful, adaptable threats – and it is this knowledge that the US government most needs from its regulatory reporting in order to make effective diplomatic, policy and military decisions. As it stands, classic "Information Security" regulations serve neither the benefit of the regulated or the regulators.

5. Lack of direct connection to risk introduction sources. Almost exclusively scoped as a technology or technology support ("User Awareness Training") suite of practices and controls, "Information Security" rarely, if ever, provides levers for or insights into how entity decision makers (such as CEO's, Procurement Officials, Agency Leadership, etc.) are creating or should be influencing the state system. Instead, they attempt to compensate or unmanage system exposure introduction and are thus subject to (likely) more externalities than they can, by definition, control.

Taken together, these and the other limitations – at a minimum – hinder progressing sustained risk reduction. By investing (and entrenching) practices such as these, entities are expending valuable financial, political and cultural capital into efforts that lock them into constraints that work against their own interests and (by themselves) limit their ability to respond to thoughtful, funded, adapting adversaries and environments. Unfortunately, this is not the extent of the problem.

Attend any conference, framework development effort or international policy workshop and elements of information security practices will have snuck in under the guise of "strategy." For example, Industry, Government and Military leaders can often be found discussing the need for better "Information Sharing" and the impacts of "Vulnerability Markets" in cybersecurity. The massive misalignment of these topics with the roles and responsibilities of those developing long term strategies cannot be overstated. It is not only inappropriate but potentially fatal to a long term success.

Why? At best, "Information Security" practices are helpful at making us better at engaging in conflict. They neither provide the levers nor address the scope of problem space required to reduce cybersecurity risk over time.

> "Information Security" practices neither provide the levers nor address the scope of problem space required to reduce cybersecurity risk over time.

Not only that, but working strategy at this level does something impressively frightening to how we think of the problem: replacing "Information Security" tactics for real strategy removed the conceptual idea that the relationship between risk owners and their adversaries is something that can be strategically changed.

By focusing all of our resources on improving the types of tactics "Information Security Practitioners" engage in, leaders inadvertently are using their authority of power to limit cybersecurity strategy in a way that perpetually escalates conflict: as complexity increases beyond what resources can combat in terms of incident management, there will be sustained resource drainage while potential consequences to accumulate over time. This provides additional opportunities for adversaries to take advantage of a connected world, does nothing to de-incentivise the use of connected system hijacking as a strategy, and does not even provide risk visibility into our nations or industries.

"Information Security" undoubtedly provides necessary suite of tools and capabilities, but it is, as a discipline, not a path to success. There must be a vision, a plan and resources allocated toward breaking the siege we are all living under online.

It is easy to see how we arrived here and examining that process helps to explain why there remains such a fixation on such low-level practices and what barriers exist to realigning our strategic discussions to more appropriate elements of the problem space. Take, for example, any of the United States' proposed "Information Sharing" bills over the past few years. Why is their congress discussing such minutia? "Information Sharing" should be the type of capability that evolves out of strategy and into law; not forced. But, here is (partially) how that conversation evolved:

Years ago, the internet was largely an island unto itself. It had the occasional security events, but they were limited in scope of effect and concern. Technologists concerned with running the internet took note, but they largely had limited scopes of influence and no real dedicated security resources. To fill the gap, they began to develop practices that they could implement within their spans of influence.

Sometime later, additional – much more publicly interesting – functionality was added to the internet. People began to care what happened in this new space. Not long after, businesses began to experience a plague of automated worms and the real value was put at risk. A market need was identified and the technologist-developed practices began to be sold as solutions. This worked for a while because the worms attacking infrastructure were thoughtless; they more closely resembled natural weather incidents than adversaries whom static defences could and would pivot around.

As the information security industry expanded to meet this need, even more of our lives became connected to the internet – along with all of our associated conflicts and crimes. Automated worms began to give way to thoughtful adversaries, but there were two key problems:

1. The automated worm solution set had become an entrenched industry.
2. Thoughtful adversaries took advantage of how we did business – they exploited flaws in our decision-making capacities throughout government and industry – not just technical flaws.

Instead of being able to adjust our perspectives and expand scope, we fell back on what we had available and were unwilling to expand the scope of security in a way that influenced how we produce value. We allowed our adversaries' scopes to exceed what we considered attack surface and we have not yet shifted out of that mindset. Worse, in fact, we have dug in our positions and have attempted to wring the very last bit of capability out of a technology centric approach.

The failure of this approach can be easily seen in the obsession with information sharing. If businesses and governments are leaving the doors and windows open on a regular basis, the only solution is for our "defenders" to learn as much about the adversaries as possible and respond using threat-centric approaches. This leads to several (hopefully) obvious problems:

1. Someone has to be compromised before we know how we might be compromised in order to have information to share. That "someone" might be us – and on a shared infrastructure internet, that distinction might even be meaningless.
2. We really can't ever know all the threats out there and, more importantly, attempting to prioritise threat information as a key component of our strategies actually ties control of our long term decision making into the short term decisions made by adversaries. This is unsustainable, if it works at all.

Yet, despite these limitations, there is a number of "Information Sharing" bills proposed in the U.S. congress and huge volumes of materials dedicated to improving it. The tactics of practitioners have

risen up into the strategic tiers of "international decision makers."

Perhaps passing a few of these tactical laws will be helpful in shifting the discussion into deeper territory. As we enable better conflict, there could be room created for a new vision into the problem space.

> "With luck, new leadership over time will look at where we are, see the failings of "Information Security" as a strategy and develop a vision for reducing cyberconflict through innovative application of statecraft to the real barriers we are facing.

With luck, new leadership over time will look at where we are, see the failings of "Information Security" as a strategy and develop a vision for reducing cyberconflict through innovative application of statecraft to the real barriers we are facing. These barriers exist, in their most critical form, as cultural, legal and political limitations to how we make decisions, work together and build sustainable, resilient human processes and systems as whole societies – as opposed to individual enclaves of the "networks."

Until this happens, and as long as we continue down the path we are on, complexity will increase, investment will become more entrenched and the risk and conflict associated with connected systems will increase. ■