The Israelisation of the Information Organization

It's not about technology; it's about attitudes and behaviours

Even the most mundane are now information *organizations and, like it or not, must operate in an increasingly hostile environment. (Cyberspace has a preponderance of terrorists.) Israel is a progressive state that has risen to the existential threats of harsh natural and human environments. In that example, we see technology will not make us safe; the attitudes and behaviour we take into the cyber realm will. We should be curious about the Israeli mindset for living and thriving in a hostile environment.*

Even the smallest and most mundane of organizations is now an *information* organization. If not operating in the Cloud yet, it is certainly online, connected to its customers, vendors, partners, and so on. This is undeniable and unavoidable. It also means that *all* organizations are subject to the pervasive, existential cyber threats of the age. Cyber risk is not just for "them" that have big or critical systems with "important" data.

If a large part of the economy and society comprises information organizations so that all businesses and individuals have to concern themselves with cyber risk, where does one start? Cyber threats aren't in some contained place "out there," so that we only need to keep them on their own side. It's not that simple any more—if it ever was.

The information organization's environment

Never minding the actor, be it a state (sponsor), organized crime, or recreational hackers, system compromise is happening in increasingly sophisticated ways. The good old DDoS (Distributed Denial of Service) attack is intended to disrupt by overwhelming a system with inbound traffic. It's like when the Ticketmaster phone lines would be crippled by fans seeking U2 or Springsteen tickets. It's a battering ram that forces a target to focus on defense at the least and on (expensive) measures to deflect this and future such attacks. These barbarians may be at the gate, but they remain outside. So the typical response is to keep them there while thickening the insulative barriers.

There are malicious Websites. Online dens of inequity where one enters—innocently or with illicit intent—and emerges with a viral infection that is unwittingly spread within the organization's own system. This applies to malicious Apps as well. All typically honeypots that are not what they purport to be. In some cases, the victim gets there actively. In other cases, cross-site scripting might have the unsuspecting user think he's doing one thing legitimately while actually doing something entirely different: like actually emptying an online bank account while apparently completing a survey or buying a motorcycle helmet.

The bigger problem is malware. This small word clothes a heap of problem. Fundamentally, malware is software code that does something malicious. It is decidedly hostile and it might come at you and your organization at any time through any path: on an infected USB key, via a malicious link/Website, in attachments to "legitimate" or spam email, and pretty much anything else essential for digital living. If data moves, malware has a channel. Malware infiltrates the system, then does *something* harmful.

What kind of harm can malware do? A rudimentary virus may cause damage to the system or launch spyware that finds—maybe records—what's going on and then exfiltrates that (private) information out of the system. With the average cost of a data breach being $4-million USD, even the least sophisticated malware creates commercial havoc.[1] Malware worms its way into the system inertly and then executes its malicious intent. Sophisticated malware has been found evolving and traversing multiple, connected IT systems. While they entered as several, discrete and harmless files, once settled inside a system and united with confederate files, they execute. Such "sleeper" malware may lay dormant weeks, months, or years.

The number of ways into a system that need to be protected is called the threat surface. The bigger the threat surface, the harder it is to protect. Though I have no factual basis for this, it stands to reason that the risk increases exponentially relative to the threat surface. And, highly problematically, the threat surface itself is expanding geometrically thanks to the Internet of Things (IoT) in all its variations. For example, in July 20 it was reported that hackers accessed and took data to Finland from an American casino. How did they gain access? Via a fish tank connected to the Internet so employees could manage it remotely.[2] Smart devices from dolls to Alexa™, tire pressure sensors to thermostats are all susceptible.

Encryption is often touted as a panacea solution. It may not be so, if for no other reason than because every tool for good can also be used for bad. First, all encryption will eventually be compromised with sufficient attention and patience. Second, stronger computing forces advances in encryption algorithms, as older versions are defeated through simple brute force enabled by more processing power. Third, if the information organization can use encryption as a means to protect its data, so can those using malware to compromise those systems and data. To that end, 33% of malware now uses encryption.[3]

The point about malware particularly is that unless resigned to wholly disrupt its operations and functioning by trying to keep "them" or "it" out there, the information organization has to learn to live in an environment that is essentially hostile. Moreover, it has to come to terms with this enemy being not merely all around but actually disguised and hiding within. The information environment has a high preponderance of terrorists. To be integrated with supply chains and customers, to be productive and effective, the information organization has to continue doing what it does fully part of this hostile environment. (After all, "If you change what you do, the terrorists have already won.")

And what's this about Israel?

Love it or hate it, as everyone knows Israel is a state created in Palestine in the late 1940s by UN fiat to provide a homeland for the nation of Israel. Despite undoubted good intent, the land at the eastern end of the Mediterranean is hotly contested as an ancestral or religious homeland by the three major Western religions. Israel's predominantly Jewish population is surrounded by states dominantly Arab-Muslim. For reasons well beyond religion, since its inception the state of Israel has existed in a continual state of actual or impending war.

The worst is there is no safe place. Every part of Israel is well within range of its neighbours' artillery. But the requirement for internationalized, open access to Jerusalem by Christians and Muslims means there are literally enemies within. For decades, Israel was ground zero for suicide bombers in the streets of the largest cities and the

[1] Larry Ponemon, "2016 Ponemon Institute Cost of a Data Breach Study," Ponemon Institute, June 2016.
[2] Selena Larson, "A smart fish tank left a casino vulnerable to hackers." CNN Money, 19 July 2017.
[3] 2016 Trustware Global Security Report.

smallest kibbutz. Israeli airplanes and ships were targets both outside and within the state's borders. Israel fought back hard, sometimes proactively, and often successfully.

Never mind the human hostility. The land itself is unwelcoming. To the north, east, and south: sworn enemies; to the west, the Mediterranean. Most of the land is desert. There was not nearly enough water for its people to drink, let alone to irrigate the crops needed to feed its growing population. The natural environment is probably at least partially responsible for Israeli inventiveness and the development of solutions to the natural and human challenges.

This is neither to indict nor to exonerate the state of Israel relative to challengers for the land. It is only to say that Israel is a productive and progressive, generally peaceful state within a harsh, even hostile environment. That reality has, among many other things, forced the Israeli character to be wary, suspicious, cautious, pragmatic… Israel did not crawl into a shell, pretending its enemies could be kept outside while it strictured itself inside. This approach to the environment extends from traditional threat into the equally existential cyber threats to Israel.

After the information age was in swing but long before the Internet brought cyber threat and terror to the broader public and imagination, and especially after 9/11, the wider Western world had to again come to terms with terrorism. Throughout America and other Western nations, airports and other public spaces were successively locked down. When airport lines in major airports dragged on for hours and the public was all but stripping naked for security, authorities turned to Israel. Ben Gurion airport in Tel Aviv had been highly secured for decades. There was obvious military presence—as everywhere else in Israel. But queues were reasonable and the airport's screening was exceeding close to error-free. The magic: Israelis had devised invisible, interlocking and mostly non-technological methods to ferret out dangerous people without the slow, ham-fisted approaches favoured by G20 nations in 2002 (and even unto now).

Applying the Israeli approach to the information age

There is obvious, reasonable precedent for examining the Israeli model when it comes to threat management. From processing travelers to managing border crossings and desalinating sea water, Israelis have risen to overcome the challenges of natural and human existential threats. Even now in the information age, the West looks to Israeli innovations that come from its military and private innovators, many of which are housed in Cyberspark, at Ben Gurion University in the Negev. The West ought to not stop with examining only point solutions to specific threats. While certainly essential, it misses the bigger opportunity.

It is the Israeli mindset and approach to living and thriving in a hostile environment that ought to dominate our curiousity. The point being that Israelis have long known their environment is not about to change: they cannot achieve carefree safety and security. Yet they are resolved to not be cowed into an ever-diminishing box of others' choosing. The only alternative is to challenge the basic principles of defense and fortification, and apply new thinking at every level from border to bar mitzvah. This is what Israel does. Its impact on the culture manifests itself everywhere from personal to business to state affairs.

Israelisation

All organizations are information organizations and, like it or not, exist in an increasingly hostile environment. One that if not lawless is nonetheless replete with international outlaws that police will remain forever chasing. We collectively need to recognize that it's not the technological solutions that will make us and these organizations—and our way of life—safe. It is the attitude and behaviour we all take into the cyber realm.

There is sufficient parallel between the environment of an information business and that of

the state of Israel. In both contexts, the enemy's intent may not be known and could evolve, identification of enemy activities could be an existential issue, and that enemy is not either "on our side of the wall or on theirs." These enemies infiltrate and attack from within. The evolution of Israeli attitude and behaviour may be a model to emulate for the information age. The approach could be valuable to apply as Canada and other Western nations contemplate cybersecurity measures and regulations; as commercial and government organizations explore means to protect themselves from cyber threats; as vendors of cybersecurity and cloud technology services devise advanced protections from evolving cyber threat.

Timothy Grayson

This and other papers are available at institute-x.org