A New Information Security Ecosystem

OUR STRATEGIES NO LONGER SUFFICE TO PROTECT US

IMPESTRA
Strategy & Performance

Enterprise Competitive Momentum - January 25, 2014

Security threats have changed in nature and frequency

Information related attacks perpetrated against companies are every day more sophisticated, less predictable. Mere hours separate the identification of a new exploit from the first full scale hacks, and in some cases the exploit is the direct result of advanced, systematic research performed by professional teams worldwide.

As the skills and expertise of professional hackers are growing, they are often supported or owned by organized crime and nation-level organizations.

The funding of such networks of cyber-criminals at such scale outpaces the capacity of any company and most governments to provide adequate protection and deterrence. With a relative impunity, organized groups can select a target and hit it relentlessly until they break in; unfortunately, there is no actual way to stop them short of taking the targeted assets offline entirely, which in many cases is practically impossible.

Those groups can afford to design and create extremely complex automats (robots) which can outsmart any existing defense through heuristics and extensive networks

The late 2013 security breach at Target was aiming at capturing credit card information and codes; unrelated January 2014 arrests at the Mexican border showed a batch of credit card information that had already been resold and was about to be used. The latency of the exploits to reach criminal organizations vanished as cyber-crime is increasingly sponsoring the creation and use of the exploits. An actual open-market for stolen cyber-goods has become normalized and operates using a model not too far from eBay and other open market mercantile exchanges.

Traditional response and response strategies are no longer adapted to the fast moving cyber-crime, and national watchdogs are nowhere close to matching the means and the skills of the newest generation of cyber-criminals. Many security practices are basically the same monolithic ones created at a time where data centers were inexpugnable fortresses surrounded with layers of fences and electric wires.

Then came smart hackers, and the realization that most of the vulnerabilities come from the inside. Either breaking through the weakest individual link (employee or contractor) or supplier / client network connect will provide unhindered access to a vast array of privileged information without much effort. There is not much a company can do to stop this, even with a world-class security. Why bother crawling on your knees and elbows to sneak into the place, when all it takes is someone to hold the door for you, willingly or unwillingly? It is then too late to stop the invader, already in the inner sanctum and who probably took all the precious information away before anyone notices… if it ever happens.

In this new world where cyber-crime is the new normal, a complete economy is being created that operates on the same traditional macro-economic rules with the sole purpose of dealing with illegitimate data acquisition, sale and exploitation. This is a global economy, involving all regions of the world, where market dynamics are based on the value of the data for sale; in this world, the boundaries between crime, espionage and terrorism are blurred and the immateriality of the buyer and seller is assured through the use of dynamic IPs and other tools enabling cyber-criminals to operate absolutely out of reach and out of sight.

We need to engage into a complete rethinking of our cyber security, not only at the defense and response strategy level, but also and more fundamentally on how we store and use the information today.

We all are targets. Nothing personal.

The Department of Defense and Wall Street firms are no longer the primary target of attacks, as ethical activists are being out crowded with espionage, petty crime and terrorism pundits.

All of us are potential targets, for small cash unauthorized transactions, identity theft, preparation for Denial of Service attacks, or even practice ground for cyber-criminal in-training. Even a small amount of loot is meaningful when repeated a few hundred times at once. We entered an age where someone will do anything for money, eventually; organized crime and rogue governments know it and are exploiting it. We better get prepared for it.

The explosive growth of social media and its multiplication of private information into the public domain provide a continuous flow of entry points and vulnerabilities, augmented with the mostly obsolete mindset regarding passwords and protective layers. Marketing dynamics and social media marketing are all creating lists of targets, laden with personal details and preferences.

Past exploits were a combination of politically or socially motivated groups such as Anonymous (Hacktivism), of nationally supported espionage to capture industrial or military secrets and of cyber-criminals trying to find a trove of information to take advantage of, such as credit card etc. Over time, the cyber-criminality has become so effective that the threshold of what makes a viable target has shrunk from a global bank or corporation all the way down to the soccer Mom with a single bank account. The use of tools and "bots" to acquire the raw data has been lowering the cost of this initial capture, which in turn is changing the economics of the hack: what would have been a low key capture is becoming a valuable target simply because it is part of a broader capture. When a single account would provide little value by itself, the association of hundreds of them simultaneously increase the returned value of the effort with a marginal incremental cost. This makes you and I become valuable targets to organized cyber-crime, when we were negligible to the individual hacker in most cases.

A disturbing thought is the blurring of the boundaries between terrorist and criminal organizations, fueled by their common never ending compulsive need for more revenue. As networks harvesting and distributing drugs are becoming less and less distinguishable from each other, when they are not collaborating, cyber-channels are taking the same path, making the definition of valuable data a lot more complex. Your bank account is no longer the only targeted information; your work related accesses, the company you keep, indirect information on companies and infrastructure can be equally valuable, as long as someone is ready to pay the price. Nothing personal, it is business.

With the commoditization and the globalization of technology networks, skills and data flows, a new economy is being born, operating under the same rules and the business economies, with the caveat that its tenets are of a criminal enterprise. Networks and logistics, national and international market places, safe heavens, schools and experts, funding and investments: all classic components of a thriving trade activity are present in the illegitimate data market. Although operating under the radar from most of us, this self-regulated economy has been growing rapidly to the point where attacks and criminal endeavors can be "profiled" by experts. This underworld is actually structured with local actors, international brokers, websites, applications and global buyers, in an entire "black" economy where the trade is information.

In this new world, we are merely passers-by, international networks, resellers and buyers, making all companies, all organizations and all of us a potential target. When Hacktivists would spend time and effort to penetrate the mailbox of the executive team of a targeted company, cyber criminals are more likely to go after a thousand of softer targets, which together create a higher return value. Teenagers being teenagers, there will always be a posse breaking into the Principal's mailbox for pranks or for tests information. But this is not really worse than climbing through the window a few years ago to get the same result. Hacking into

John Smith account to get banking routing numbers and sell them to a gang operating outside of the borders is not driven by anything but elementary demand-supply market dynamics, where volume and usability are becoming the core criteria.

Shifting the security focus

The responses to these new threats need to be in almost-real time to be meaningful, and make the breach sufficiently difficult that the effort required creates natural deterrence. One positive thing about cyber-crime's reliance on automated tools is that sufficient complexity in the fencing security (like a very strong password) will exhaust most tools' scripts before breaking in, creating de facto deterrence. There always is the case of the hacker-in-training rising to the challenge, but mostly professional crime is driven by profit and a common business practice is to drop cases you cannot win easily….

Meanwhile old core security strategies of doing periodic assessments and monitoring randomly for threats analysis are no longer sufficient to protect a company's data. Some of them even contain their own Trojan horse, as the focus remains on creating a very difficult to breach first barrier behind which everybody feel – falsely – safe; when this barrier fails, no protection whatsoever remains, leaving the critical data fully exposed.

Internal security experts (the good guys) are themselves facing the unique challenge that new generations of cyber-criminals are coming up continuously, each of them outpacing them a little more in their skills and capabilities. The training and constant watch of emerging threats and exploits is the new battlefield for Cyber Security experts, so they can at least keep up with the fast evolution of the attack strategies. This is a losing battle however, as long as experts protecting companies and our society are stuck to a reactive mode. The emergence of a new class of threats continuously evolving to defeat barriers being raised requires a whole new thinking on security strategies, as deterrence is becoming an economic barrier and no longer a security frontier.

So here is the dose of reality: it is no longer credible to assume that you can find a set of security barriers and responses which would stop all attacks. Over time, your best defense will be defeated, given enough attention and desire from the bad guys. Let's absorb the implications of this statement for a moment…

The old concept (still very much the only one at play for many companies and organizations) stood on the foundation of a strong, active set of barriers and alarms protecting the core information stronghold. This is also the model of medieval fortifications, highly effective until modern warfare turned them into tourist attractions. As initial deterrence remains an important disposition of the security apparatus, it created an associated flip side, with all key information and resources completely unprotected would someone breach those barriers. Until a hostile penetration occurs, nobody worries about being exposed, feeling comfortable behind the tick walls of corporate security.

Suddenly there is a breach and they are looking in the eye of a hostile bot with utter panic, the best option left being taking the entire organization offline, if this is even still possible, and provided that the threat is not discovered days or weeks later.

The focus of an effective security strategy can no longer be limited to a series of electronic barriers that creates a treasure trove of data for the intruder. It leaves critical data fully exposed to hostiles breaking through. CISOs and other Security architects need to cover all fronts simultaneously, assuming that each of them can be breached. A perfect illustration of the new thinking is when an organization digests the fact that most of the breaches are originating with insider knowledge, shared deliberately or unwillingly with someone who then takes action.

It is practically impossible to prevent all employees from surfing into unsavory internet sites, respond to phishing campaigns, store key passwords on their smart phones and so many elementary security protocols violations. It is sometimes puzzling how people otherwise mature and savvy can be caught red handed protecting critical information with John123 or their birthdate as the password (when it is not just "PASSWORD").

Adding to this the pure data leakage such as the credit card information of customers left on a non-encrypted laptop forgotten on the back seat, or the deliberate industrial espionage tools to capture encryption keys, there are too many weak spots to effectively protect all the data all the time. It is therefore a new reality that we are facing, where strategies and tools need to be built to separate data or architect it in ways that accessing to a data store would only give a partial, ideally worthless view of the core information.

Let's assume that someone will be able to access your core customer information, sooner or later. The question is how to make sure that this access will not provide access to enough aggregated data that makes it become a marketable merchandise for electronic pirates and their customers. Separating logical strings such as the contract terms and conditions from the name and mail address, or splitting the customer base in subsets without universal access can illustrate what a "disruptive" data architecture could be. Using hard encryption on key data sets without which the rest of the data would lose a lot of its value could add to the difficulty and make it more difficult (hence require more efforts /costs) for cybercriminals. In effect, the goal here is not to prevent access (which is another simultaneous strategy) but to make complex and hence expensive enough to re-aggregate the data into a trade worthy loot, rendering the acquisition not profitable enough for the potential hackers.

What is missing is a multi-prong strategy including a dynamic response to ongoing threats, and a whole new philosophy on critical information and storage.

A new thinking for a new class of threats

A dynamic response is basically a set of tools above and beyond the usual cyber-security barriers, continuously checking and analyzing the flow of activities in the entire network, to flag single events and abnormal behaviors as soon as they occur.
This activity should be automated as much as possible, and smart tools should be leveraged to start matching the cunning talent of cyber-criminals with comparable smarts.

Besides an alert system flagging transactions, flows and patterns as soon as they arise, human oversight should continue analysis and observing traffic patterns to continuously evolve the knowledge embedded into the early warning system. Creating networks of guardians sharing information and tips as

they emerge, the collective response would grow significantly, along with a direct reduction of the potential impact of a new penetration routine. National Cyber-Security watchdogs would also be able to provide inputs, as well as benefiting from the broad network of individual custodians of corporate security (national and federal organizations being chronically under-funded and ill-prepared for taking on such broad coverage).

The primary benefit of an early warning system is that you can catch a threat as it occurs, and before too much damage is done. Needless to say that the earlier the catch, the less repair and cleansing will be needed, but it also enables to shut down the backdoor fast, as well as being able to capture the details of the penetration threat and therefore get a much better sense of where it comes from and how it got around the first perimeter of fencing. This must remain a learning system, not a static moat.

A secondary benefit is to fine-tune the early warning system itself, enabling it to catch earlier signals and outsmarting more covered "agents", eventually matching closely the creative skills of the new generation of hackers.

A second and equally critical component is the complete overhaul of the data and information architecture within the organization. Today's IT organizations and architecture are primarily designed from the vantage point of Technology being the custodian of Corporate's data. While this situation has historical merits and rationale, it truly did not evolve much over the past decades, creating huge repositories of original data in massive technology silos. The classic alternative of having individual users create and store their own data being an even worse scenario, nobody has been effectively questioning the fitness of such architecture in an increasingly online and virtual world. There lays the fundamental issue: the very concept of data custodian, central to most organizations, is generating fat sitting ducks for cyber-hunters on the prowl. Would one of them breach the cyber-fences, and the entire set of critical and non-critical data is just there accessible with almost no stopping.

Some organizations have been building layers of access filters, such as banking and healthcare for instance, mostly for regulatory purposes. But most of such barriers were designed to prevent end-users from accessing the privileged data, leaving technology access mostly unchecked even if monitored. Companies need to rethink their entire data strategy with the clear goal to prevent and at least reduce the potential access to the core information, including breaking down the most critical data into subsets meaningless unless all parts are present in the same time. Hard encryption of some of the data with dynamic keys would also build a strong deterrence for would-be hackers. Anything that makes it more complicated, call for more resources to access meaningful data is a step in the right direction.

Getting started…

As mentioned before, cyber-crime has turned into a business. Unless you are facing ethically or politically motivated hackers, there is a numbers of threshold of cost and complexity which will eventually turn off most tentative petty hacks. If you are a "professional" hacker and are looking into a couple of hundred targets, it is very likely that you will go first and foremost after the ones that are easier to grab and break. Then you would go after the next ones, and the next ones, until you have exhausted the list or reached a point where the targets are not juicy enough to justify a continued efforts, while other sitting ducks are quacking for attention all around.

This is clearly not a good enough strategy if you are the Pentagon, the CIA, General Electric or Microsoft, as the thrill for the challenge and the "trophy" can be sufficient to trigger passionate focus. But who would get obsessed with hacking the customer list of an engineering company designing guides for industrial conveyor belts?

Companies, and for that matter individuals too, should think hard on which private information is really critical, and how they could break it down into meaningless subsets, or protect the most critical parts if separate ways. The same three prong strategy should be used in all cases:

- Maintain the currency of cyber-fences to reduce the exposure to the outside world and make more cumbersome and costly to reach the actual first data stores,
- Revise the data and information architecture to eliminate massive data stores, create physical and logical separation between complementary data objects; create disruptive / distracting
- Establish dynamic monitoring and responses to emerging or identified threats, including actively participating and contributing to specialized user groups to keep current knowledge on threats and responses that work best.
- Sign-up or create a User Group focused on cyber security, preferably which has an official endorsement or is collaborating with secure entities such as the FBI Cyber Crime task force or Working Group, including the National Cyber Awareness System to get updates on threats and responses.

An organization enabling its employees to store credit card information on a laptop or mobile device is no different from those publishing on Facebook that they will be vacationing in South America for the next three weeks, leaving their house empty and unprotected. These are just typical sitting ducks. Would you leave on a connected computer with a folder called "Personal Data" containing a scanned copy of your ID card, passport, social security, credit cards and codes unencrypted? Then why would you leave your customers or trade secret information open for all to see?

With the irruption of Big Data, a new dimension of vulnerabilities exists that pretty much breaks some of the old walls: organizations import massive data loads from mostly unchecked sources, in order to perform analysis of patterns and correlations. The capacity of such process to generate new "exploits" for cyber-criminals is simply staggering. How many companies however have been pro-actively analyzing the very process of data mining and acquisition to create new logical fences and ensure that this data does not carry some nasty content with it? How many have been considering how competing companies could very well publish knowingly erroneous data to simply mess up the data mining process of unsuspecting data sourcing teams?

Since the actual extract and formatting of the data is the primary driver for creating value here (as data itself is readily available to all), companies should create a whole new architecture that segregates the actual external data repositories from the extracted "value added" data resulting from the process. Moreover, this data should only dynamically be combined with internal data to generate the final layer of mining and analysis, reducing the critical data availability to a time window as narrow as possible. Such data architecture would disrupt cyber criminals and make it harder to aggregate the information in a meaningful, commercially viable way.

We all have to assume that every piece of non-public data is a potential value target for criminals, and needs to be protected with a combination of fencing and disruptive data architecture and storage.

This might help jumpstart building or upgrading a comprehensive technology and information security for the enterprise. It will help get started, but will not replace being alert at all times, and creating network of security intelligence to counter the power of cyber-crime and keep up with the fast emerging new threats.

Chief Security Officers are starting to face the same issues CIOs have been dealing with in the last decade: end-users and businesses resent having to work under constraints, and it can be exhausting to always be the one to say "no". It invariably ended with the users taking the power back and forcing CIOs to catch up scrambling; mobile computing and BYOD are good examples of failed attempts to control business users through non-collaborative techniques. We need a more engaged, positive and dynamic approach to Enterprise Security.

These strategies are foundations for a new thinking of corporate and individual cyber-security. After years of leaving in fear like sitting ducks, it is time that we take back the initiative in fighting cyber-crime with the tools of this century.