The Cyber Criminal Value chain- mirrored by business risk and compliance in the 21st century.

2016

While the concept of reasonableness is somewhat subjective, the questions for CISOs to ponder are these: Does my security program constitute reasonable protections for a company in my industry and would the legal system agree? If my company is breached, and I have to explain my actions a year from now in front of a court, will those actions show that I did what was reasonable to protect my company's information assets? The cyber-threat map is always changing and so is the criminal value chain.

Just as with traditional enterprises, those operating in the underground market are driven by supply and demand. The more obscure a tool or information is, the more it is worth. Conversely, when the market is flooded with goods then the price per unit goes down.

These businesses do not operate in a hierarchy like a traditional enterprise but function more like a market-driven fair economy of buyers and sellers, each of which works as an independent contractor providing value to the community. These contractors can choose their working hours and often work a separate job to supplement their activities.

The underground cybercrime community is built on anonymity, and this anonymity can actually provide a radically free market system. The actors are only known by their handles and their true identities remain hidden. This breeds a strong paranoia throughout the business. Trust and a good reputation are key to the industry. If you are not trusted, it is very difficult to make money in the system. Trust is built by demonstrating your hacking skills, having other members of the community vouch for you, and providing valuable goods to the community.

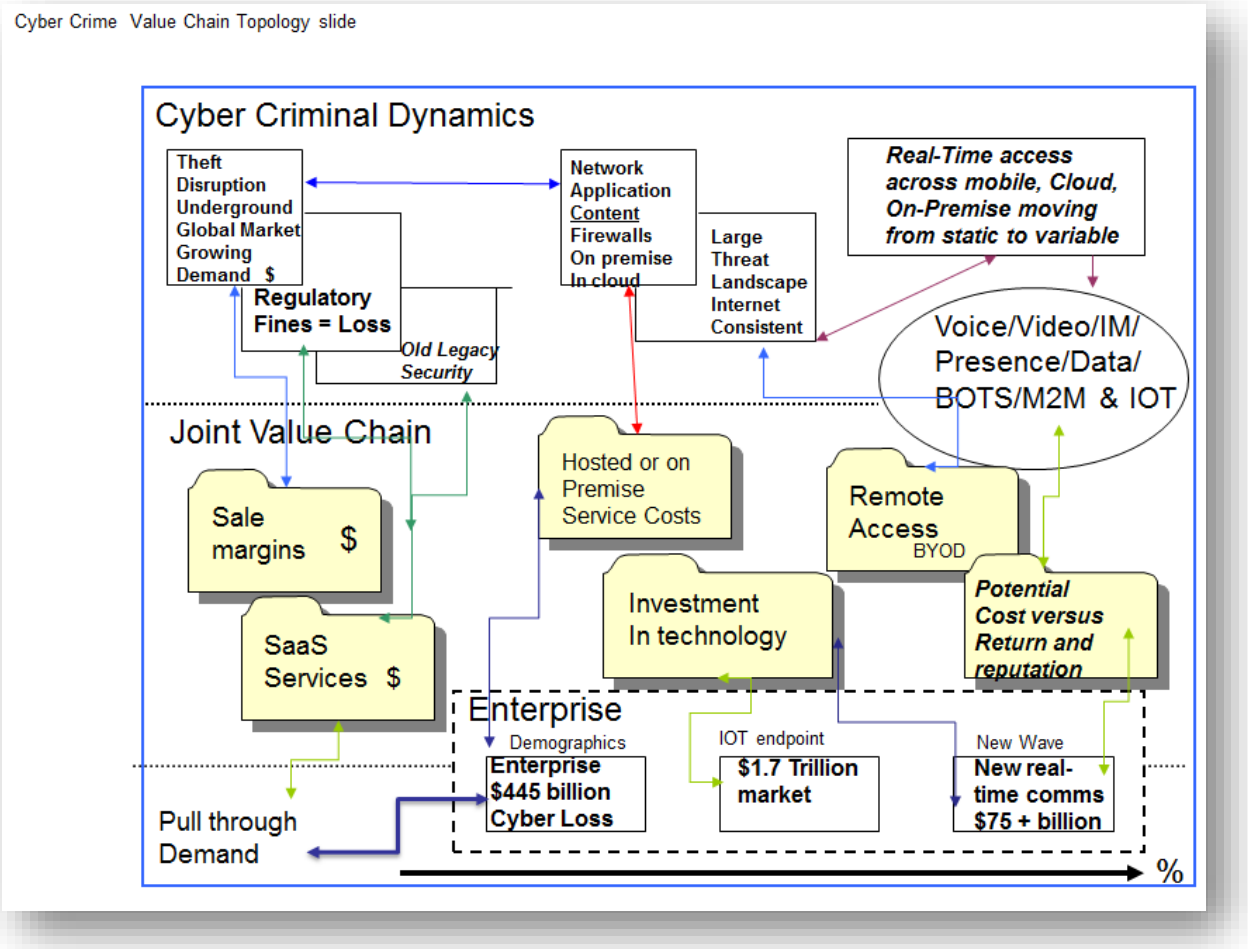
As the Enterprise Boards wake up to the reality that they are now sandwiched between the underground market and the regulatory environments, backed up by government and trade departments, pressure is mounting to a point that there is no easy way of doing business and it becomes another form of competition to maintain profits and growth.

The mirror reflects the result and the challenge is entry versus non entry, when a business recognises what its competitors are up to, they look to defend or step up activities and hopefully increase revenues, so what of Cyber Security?

To truly disrupt the business of hacking is to increase the cost of the attacker's business, erode their profits, and increase the time it takes to successfully execute an attack and sale. Think of it as competitive analysis, it is our duty as a legitimate enterprise to introduce these technologies to disrupt the business of hacking on a continuous basis. It is critical that an enterprise determine which technologies will be most effective at disrupting the adversaries targeting their unique business.

A value chain is a set of activities performed in order to deliver a valuable product or service to the market. These activities are carried out by subsystems that take an input, process it in some way to enhance value, and provide an output. All these activities together give the output more added value than the sum values of the individual activities. The effectiveness of the value chain determines the cost of the output and affects profits.

The series of activities in the value chain of the business of hacking are not under an organizational umbrella like a corporate enterprise. However, they are all pieces that contribute to the end product. This is a deeper look into the primary and support activities involved in “the business.”



Some hackers carry out multiple activities while others are highly specialized, which may lower their risk of being digitally identifiable (lessen your footprint). Specializing in a small number of activities lowers the hacker's footprint but can make them rise above the crowd and increase the risk of catching the attention of law enforcement officers.

Specialized usually means more expensive services, when a hacker can target and pinpoint network entry, create disruption to achieve open door access, move to a core application and then extract content that has a value, they have sourced their ingredients/materials to sell.

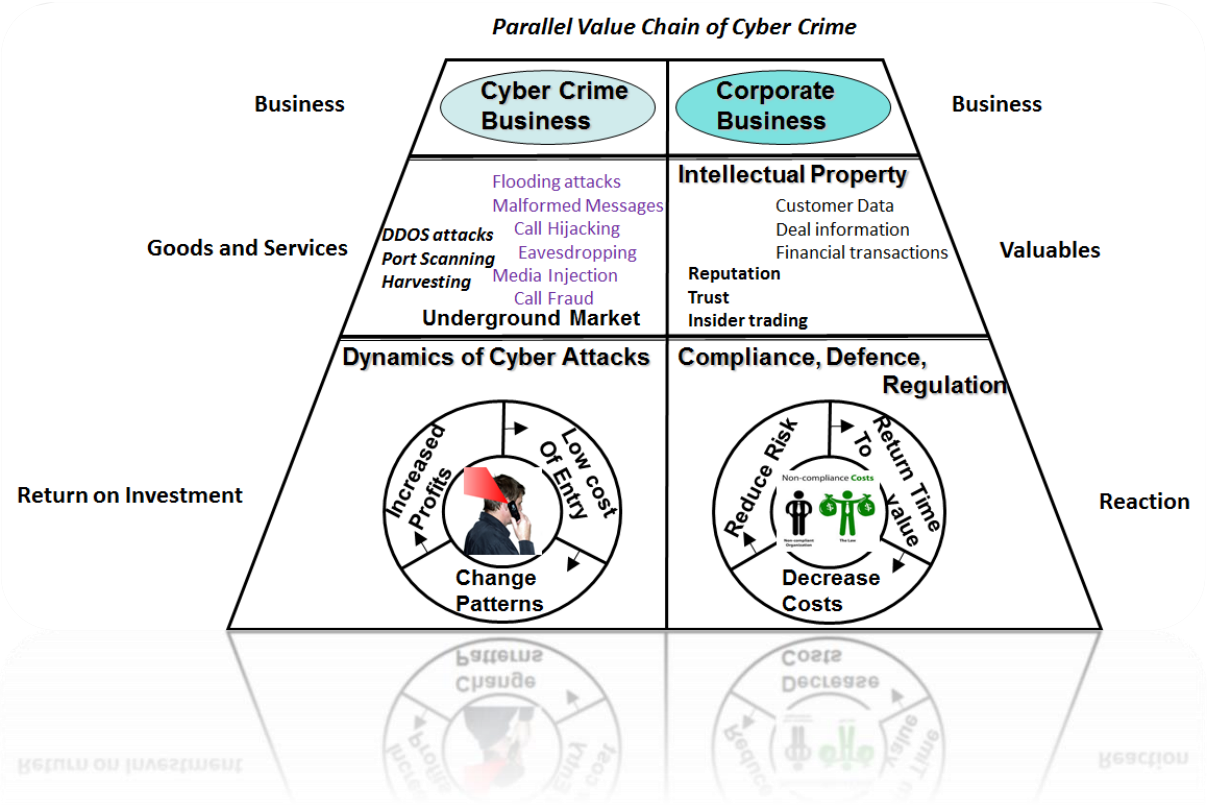
As an example, IP theft, this business involves stealing intellectual property from a target. Such activity has been seen in the electronics industry (smart phones, tablets, IOT), as well as in the defence industry (war planes, weapons, etc.). It has even been seen in the entertainment industry (movies, software, etc.). Attackers make money by either being "employed" to infiltrate the organization in order to obtain access to the targeted IP and sell it to the target's competitors.

By understanding the business aspects and drivers of hacking, we can begin to disrupt the players and the marketplace. The goal is to make it more expensive for these businesses to operate and/or increase the risk beyond acceptable levels for the attackers. Typically, enterprises must achieve this by introducing new designs for 21st century security technologies into their environments, that are created with the value chain in mind. These products may not stop attacks altogether, but they do slow attacks down and increase the cost of carrying out an attack, thereby reducing the scope for attack.

Another example is the two categories of call fraud. The first is the obvious one of making calls at someone else's expense. The second and by far the most serious is *premium rate fraud* also known as *international revenue sharing fraud* (IRSF). Premium rate fraud occurs when a fraudster sets up a premium rate number, locates a poorly protected IP connected phone system and then forces that phone system to dial the premium rate number. The fraudster then collects a share of the premium rate fee. This equated to $4 plus billion in global losses in 2015.

New changes in the market place are amazingly open, research showing that DDoS attacks have become a commodity, and are available openly on professional services online marketplaces for as little as $5 an hour, say security researchers. This is in marked contrast to just a year ago when DDoS services were typically available on the dark web for an average cost of $38 an hour, demonstrating that DDoS attacks have become a commodity.

One of the strengths of the business of hacking is that it is widely an open source community. Tools are shared, allowing for speed in gaining access to victims and in developing new exploits. It also results in a highly resilient marketplace. If authorities shut down an underground site, another one will take its place. This speed is often something our organizations cannot match. Legitimate enterprises must also abide with regulations while attackers do not. Moreover, while most countries now have cyber security laws, many of them lack proper enforcement. For these reasons, hacking businesses benefit from a large talent pool and enjoy an even larger target pool.



In December 2014 and again in 2015, ENISA published a set of technical guidelines, with which an organization can implement processes and security measures that comply with the legislative requirements for the security of electronic communications of the European Union. HR 1770, the Data Security and Breach Notification Act of 2015 in the USA along with the EU Directive 95/46/EC, now the new General Data Protection Regulation in Europe, presents major milestones for Cyber Security compliance. It also requires service providers, Enterprise in high risk areas (finance, govt, Oil and Gas, Health etc.) and their service providers to alert breaches of data to the authority list within 72 hours in Europe. If found to have not aligned to the guidelines on security technology defences and compliance rules, a fine of up to 4% of annual turnover is attributed to the increased costs of doing business.

The opportunities for hacking businesses are very similar to the opportunities for legitimate organizations. The difference is that legitimate businesses are moving to mobile technologies, SaaS, and growing economies to grow our businesses. Attackers view these emerging technologies as opportunities for weaknesses in our organizations that they can exploit. Developing countries are adopting new technologies to pay bills and access the Internet. Unfortunately, these new technologies and developing infrastructures do not always employ the most advanced security making them an easy target for attackers.

Each type of hacking business follows a typical maturity curve. There is an emerging phase where the cost of doing business is high, then a growth phase where automated tools flourish and profits increase. The mature phase follows where innovation slows, profits are steady, and typically, the market begins to be flooded. The final phase is a declining phase. This is caused by a saturated market or by new security technologies that make the hacking business no longer viable.

The number of threat targets for attacking is huge and expanding rapidly with mobile devices and outward facing sources to attack, such as the Internet of Things. There is multi-layered software defined networking designs created after research and development, that represent a new way to deploy security tactics that can be employed to drastically reduce this vulnerable target pool over the three compliant layers, network, application and content, which must all be integrated in any attack, all based on value chain rules of engagement.

The risks of connecting any data application server to public IP networks have been well understood for some time. These risks lead to the growth of the Firewall market in the early 1990, followed by the development of application specific security controls for Web, Email and other applications.

Unfortunately, there is a lower level of understanding of the risks associated with real-time communication applications using SIP, IPV6 protocol in IOT, ORTC Web which extend into based Unified Communication and Internet of Things.

As a consequence, development of application level security controls for real-time IP based services has not kept pace with the increasing risk. Many providers continue to rely on Firewalls, VPN, Application Gateways, Session Border Controllers (SBCs), Content proxies to deliver security for network, application and content, via OTT and SIP trunk services in a real-time communication world. None of which have even heard of a value chain for Cyber Crime or the rules of this engagement, so static development huge in legacy with no adaptability!

A recent pen test and compliance test showed that all SBCs are demonstrably unable to protect against many of the application level security threats faced by SIP based UC applications and services. These threats include break-ins which enable attackers to make calls via compromised systems leading to costly call fraud or using DDOS open up to more valuables.

Cybercrime cost the global economy an estimated $445bn in 2015. It also estimated by the industry that 150,000 European jobs were affected by cybercrime in the year, as well as 200,000 from the US.

Researchers collated estimates of both indirect and direct costs from governments and security firms, including loss of intellectual property, financial assets, and sensitive information, as well as missed opportunity, and the costs of protecting and recovering from cyber-attacks.

Financial losses are growing. David Burg, PwC's Global Cybersecurity Leader said cyber criminals evolve their tactics very rapidly and the repercussions of cybercrime are overwhelming for any single organisation to combat alone. The survey found that the US organisations are more worried about cybercrime compared to their global peers with 69% of US respondents reported they were worried about the impact of cyber threats to their growth prospects, compared with 49% of global CEOs.

Still Cyber Security has to be compliant and assured, it must also be delivered fast and implemented across technology platforms, and in this it must deliver both mobile and fixed security.
Forward thinking and unique to Multi-Level Cyber Security is the R&D company UM-Labs, who's founders threw away the traditional legacy and static approach to Cyber security in a real-time world, having worked with the value chain that makes this market mirrored, the answer is about aligning a service run and sold via hosting and service providing partners.

The UM Labs Real-Time communications service platform is designed for deployment in public and private clouds. This ability means that the platform can be deployed wherever needed to implement effective security controls.

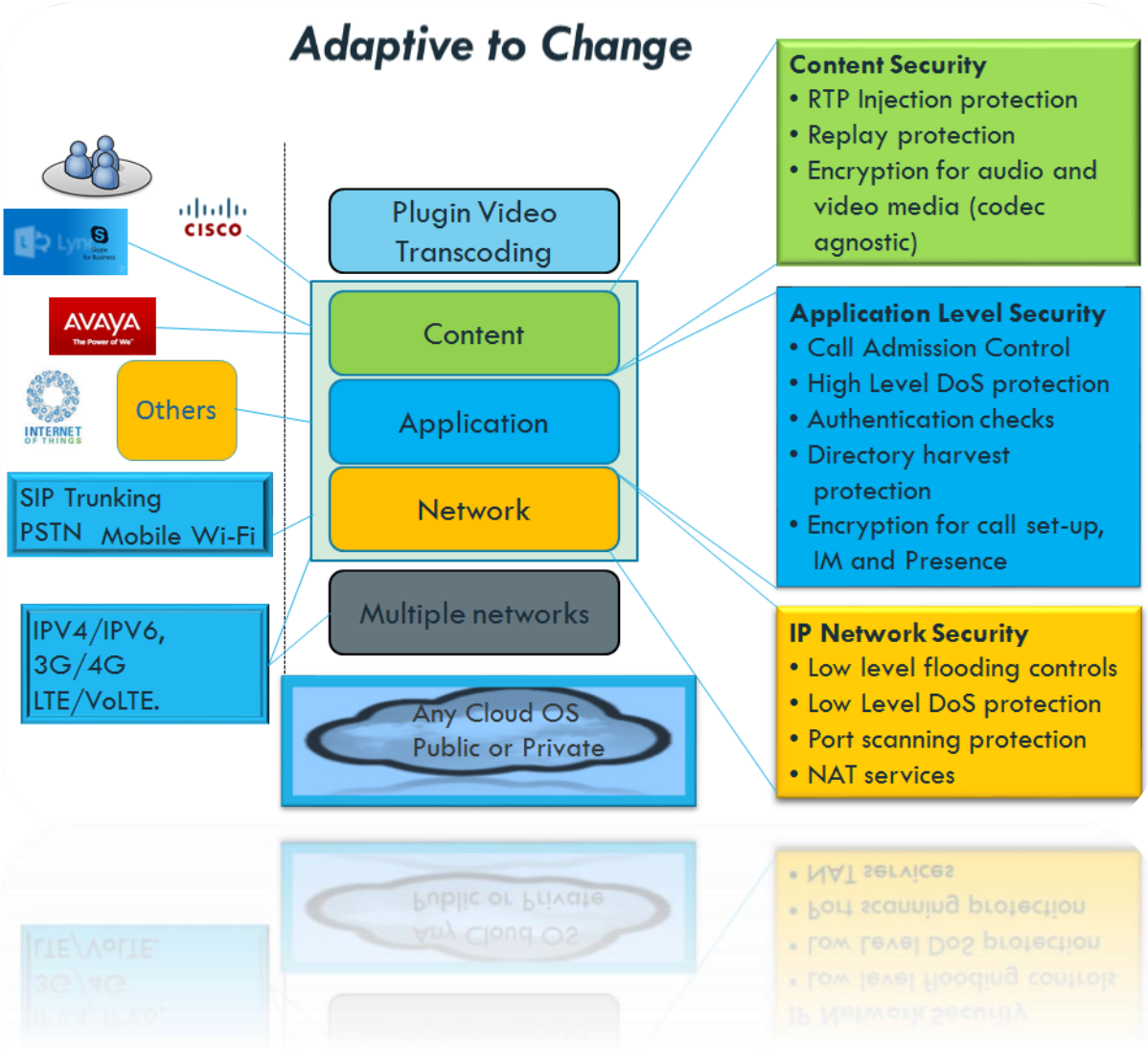
As an example a SIP trunk provider may choose to deploy the platform in their data centre to ensure that their core systems are protected. The provider may also recommend that the end-user deploys the UM Labs platform in their own data centre. The SDN design and NFV options provided by UM Labs simplify this. Deploying two systems in this way means that all SIP trunk connections between the provider and the end user can be authenticated and encrypted.

The system deployed in the end-user network can allow remote users to connect to IPPBX of any SIP make and SIP based UC services without exposing those systems to the risk of attack.

The company unique and tested platform is certified compliant by govt and Telecom regulated authorities, pen tested by Deliotte Red Teams, set against ENISA and EU GDPR rules, with compliance assured for operating over multi-levels of attacks with an integrated and adaptable to change architecture.

The licensing policy for the UM Labs platform is based on the total number of users. This means that deploying multiple systems to protect the same group of users does not increase the licensing fee.

The UM-Labs stack by its design can sit in any cloud implementation for fast, easy implementation, minutes to protect 1000's to 100,000's of exposed users begins to reduce the market place for Cyber Criminals.



For more information, contact WWW.UM-LABS.COM or Marketing@um-labs.com