RISK

cyber quotient

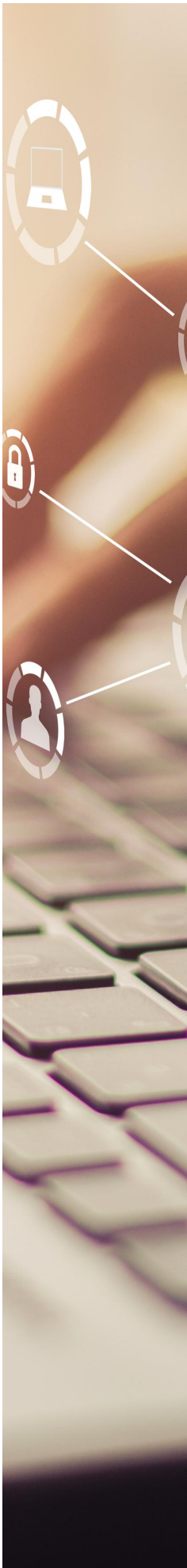
REDEFINING RISK MANAGEMENT

Risk | Costs | Benefits & Threat Models

By Team Cygularity

As humans we are driven by risks and threats, and where we are continually weighing-up costs and benefits. A threat is the actual thing that could actually cause harm, loss or damage, whereas a risk is the likelihood of a specific threat happening. Those who are successful in their lives are often those people who can best understand threats and assess risks. IBM is one company who has managed to succeed within the computer industry for over 100 years, and where they have continually faced with new threats from competitors and from the rise of new technologies. Each time they have generally managed to understand the risks that they face and overcome them. In the 1960s, for example, IBM had a lead in the market place for mainframe computers, but the 1970s saw the rise of the microprocessor and the personal computer (PC). And so IBM addressed this by adopting the rise of the PC and eventually leading with their own standard. As the development of the PC
quickened, they again they found their leadership under threat and decided to concentrate on high-end workstations and mainframe computers.

In our lives, too, we expose ourselves through vulnerabilities, and which are our weaknesses, and which could be exploited by others. Within Cyber intelligence we must thus need to continually understand our threats and vulnerabilities, and weigh up the risks involved. With finite budgets for computer security, and we must thus focus on those things which will bring the most benefit to the organisation. A major challenge is always to carefully define costs and benefits. A CEO might not want to invest in a new firewall if the justification is that it will increase the throughput of traffic. Whereas a justification around the costs of a data breach, and an associated loss of brand reputation might be more acceptable for investment.



Risk | Costs | Benefits & Threat Models

By Team Cygularity

Threat analysis is growing field and involves understanding the risks to the business, how likely they are to happen, and their likely cost to the business. Figure 1 shows a plot of the cost of risks against the likelihood. If there are low costs, it is likely to be worth defending against. Risks which are not very likely, and which have a low cost, and also a risk which has a high cost, but is highly likely, are less likely to be defended against. At the extreme, a high risk which has a low likelihood and which has high costs to mitigate against is probably not worth defending against. The probabilities of the risks can be analysed either using previous experience, estimates, or fromstandard insurance risk tables. Figure 2 outlines an example of this.

Loss Expectancy

The investment in cybersecurity must often be justified, especially in the benefits that it brings to an organisation. For audit/compliance reasons, a company must often prove that the match the key regulatory requirements within their market place. Regulations such as GDPR, and acts such as Gramm-Leach-Bliley (GLB), Sarbanes-Oxley (SOX), and the Computer Fraud and Abuse, are often a key driver for investments in cybersecurity, as a failure to comply with these can lead to significant fines or even criminal charges. The GLB Act outlines the mechanisms that financial intuitions can use to share customer data. And, due to the financial scandals of Enron, WorldCom, and Tyco, SOX was passed in 2002, and which defines the methods used to implement corporate governance and accountability. One driver for cyber intelligence is thus the ability to gather the required information for auditors to review.

As previously defined, there are many other costs that an organisation may face, including the loss of business, brand damage, and a reduction in shareholder confident. One method of understanding the cost of risk is to determine the single loss expectancy, which is calculated from:

Risk | Costs | Benefits & Threat Models

By Team Cygularity

CQALE = AV x ARO

and Where ALE is the Cyber Quotient Annual Loss Expectancy, ARO is the Annualized Rate of Occurrence, and V is the value of the particular asset. For example, if the likelihood of a denial-of-service on a Web-based database is once every three years, and the loss to sales is $100K, the CQALE will be:

CQALE = $100K x 1/3 = $33K per annum

This formula assumes that there is a total loss for the asset, and for differing levels of risk, an EF (Exposure Factor) can be defined as the percentage of the asset damage. The formula can then be modified to:

CQALE = AV x ARO x EF

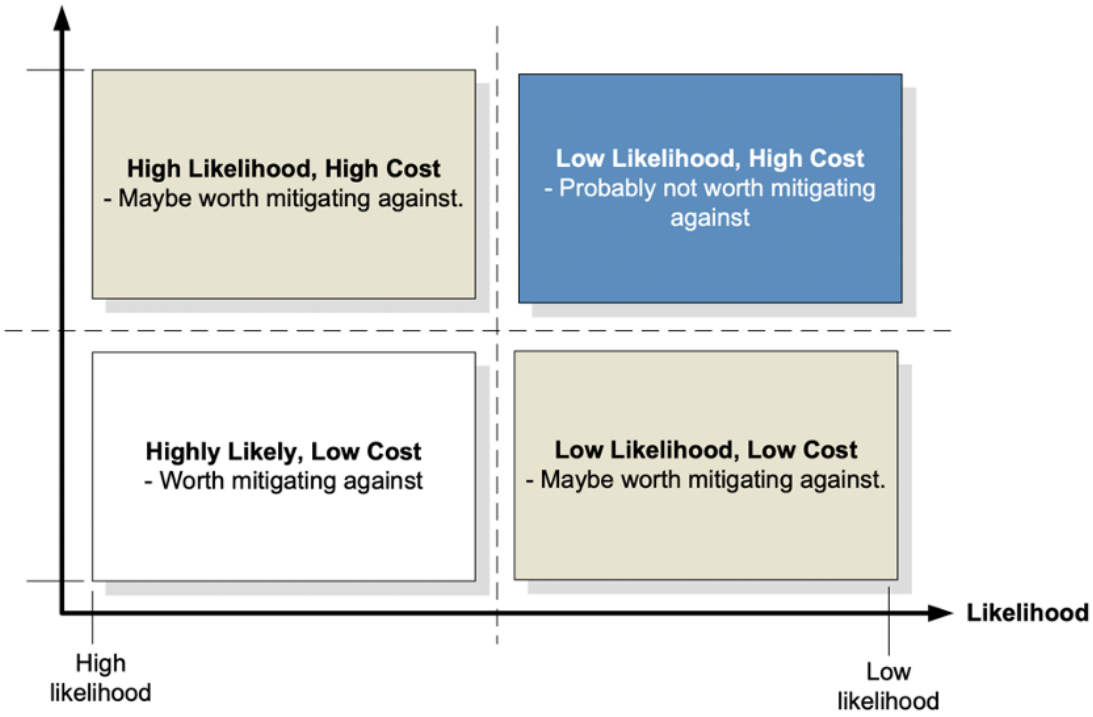


Figure 1

Risk | Costs | Benefits & Threat Models

By Team Cygularity

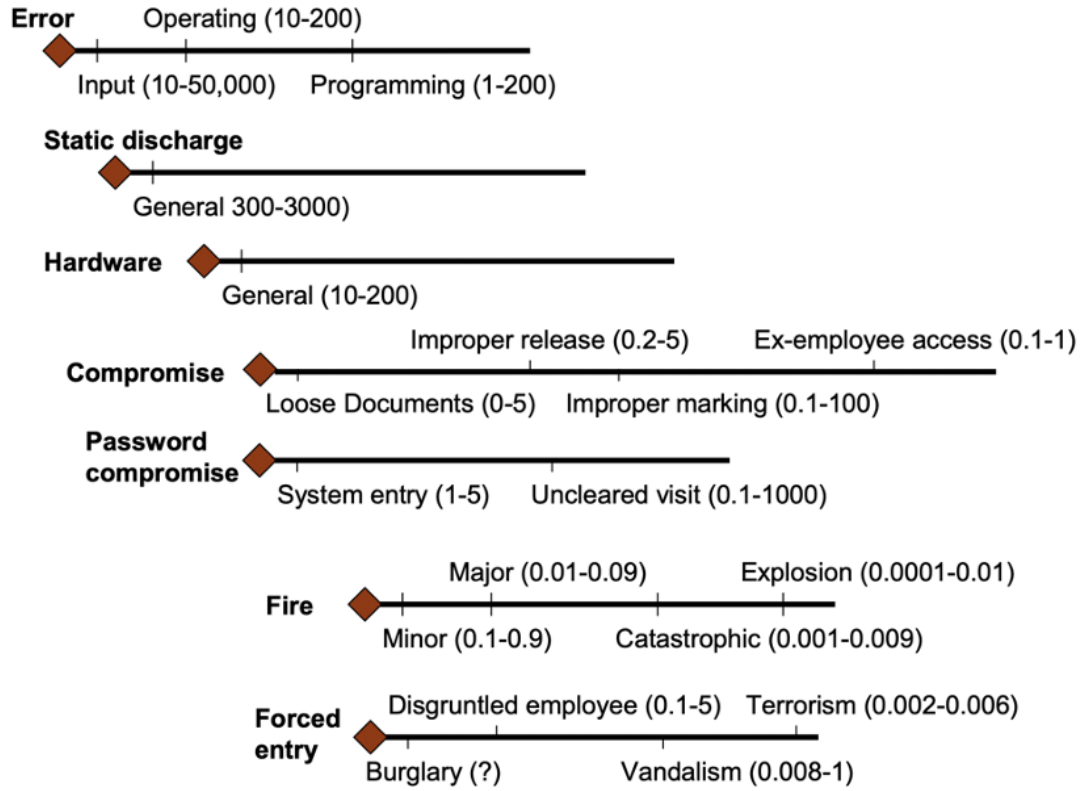


Figure 2

Risk management/Avoidance

The major problem in defining risk, and in implementing security policies, is that there is often a lack of communication on security between business analysts and information professionals, as they both tend to look at risk in different ways. Woloch [1] highlights this with: Get two risk management experts in a room, one financial and the other IT, and they will NOT be able to discuss risk. Each puts risk into a different context … different vocabularies, definitions, metrics, processes and standards.

At the core of Cyber intelligence is a formalisation of the methodology used to understand and quantify risks. One system for this is CORAS (A Framework for Risk Analysis of Security Critical Systems) and which has been developed to understand the risks involved. A key factor of this framework is to develop an ontology (as illustrated in Figure 3) where everyone speaks using the same terms. For example

Risk | Costs | Benefits & Threat Models

By Team Cygularity

A **THREAT** may exploit a **VULNERABILITY** of an **ASSET** in the **TARGET OF INTEREST** in a certain **CONTEXT**, or a THREAT may exploit a VULNERABILITY opens for a RISK which contains a **LIKELIHOOD** of an **UNWANTED INCIDENT**.

In this way, all of those in an organisation, no matter their role, will use the same terminology in describing threats, risks and vulnerabilities. For risk management, it is understood that not all threats can be mitigated against, and they will be carefully managed and monitored. Figure 4 shows the methodology used by CORAS in managing risks, and where a risk might be accepted if the cost to mitigate against it is too high. Network sensors can thus then be set up to try and detect potential threats, and to deal with them as they occur. For risk avoidance, systems are set up so that a threat does not actually occur on the network. An example of risk management is where a company might not setup their firewalls to block a denial-of-service (DoS) attack, as it might actually block legitimate users/services, and could thus install network sensors (such as for Intrusion Detection Systems) to detect when a DoS occurs. With risk avoidance, the company might install network devices which make it impossible for a DoS attack to occur.

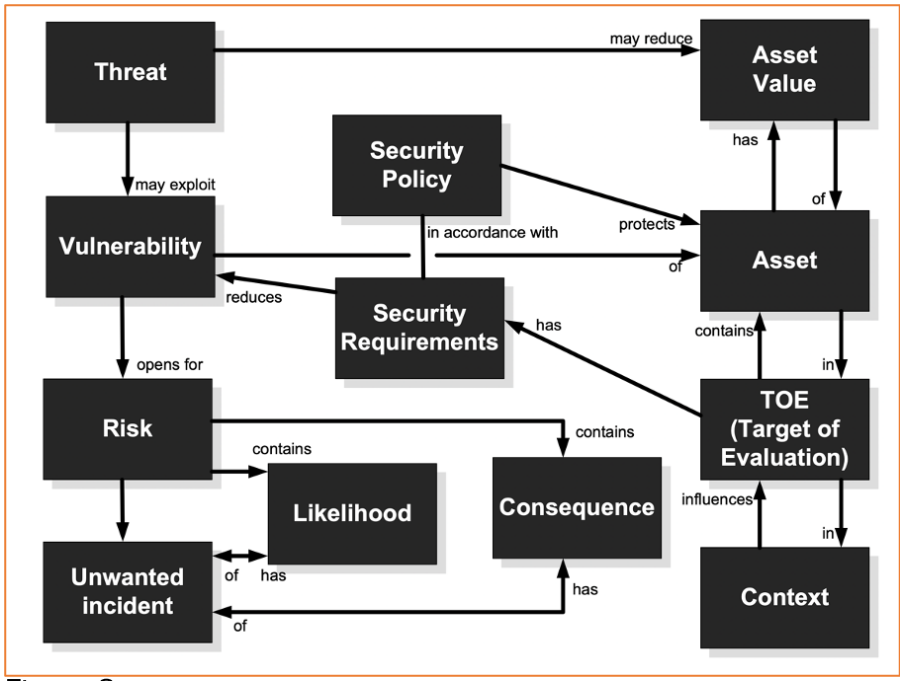


Figure 3

Risk | Costs | Benefits & Threat Models

By Team Cygularity

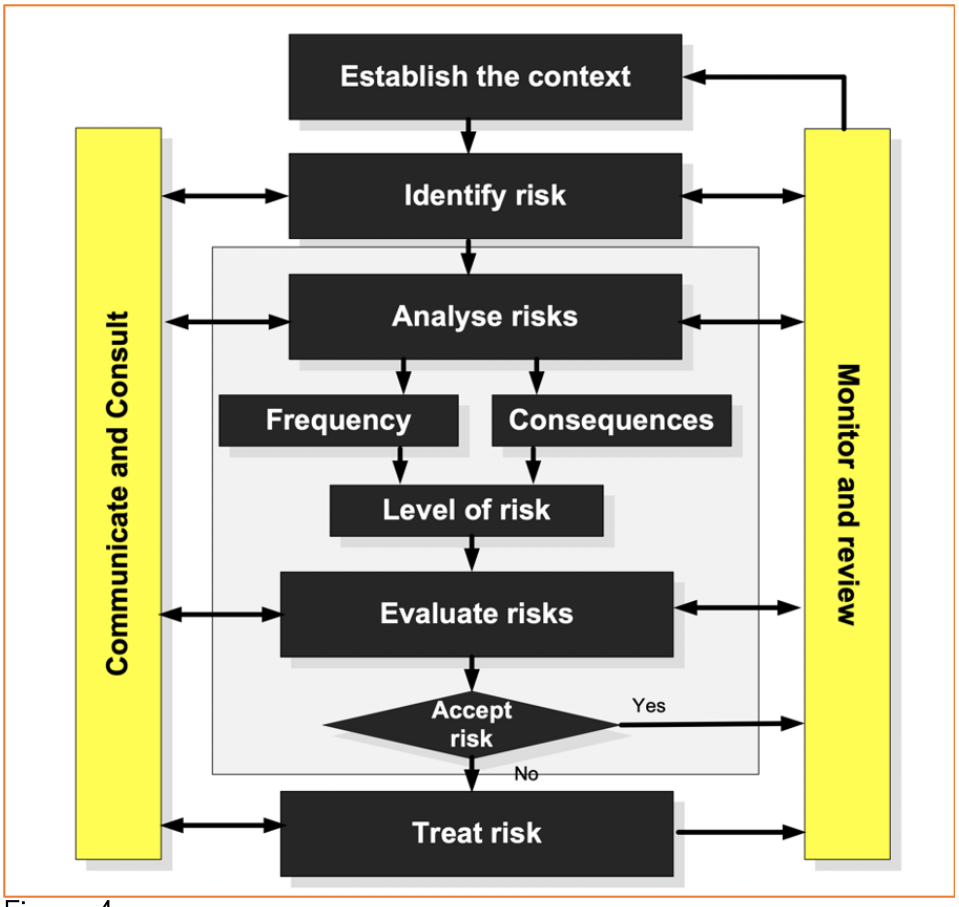


Figure 4

The importance of clearly defining threats allows us to articulate both the threat itself, and also define clearly the entities involved with an incident. Figure 5 shows an example of defining the taxonomy used within a security incident, and where: **A [Threat] is achieved with [Attack Tools] for [Vulnerabilities] with [Results] for given [Objectives].**

Risk | Costs | Benefits & Threat Models

By Team Cygularity

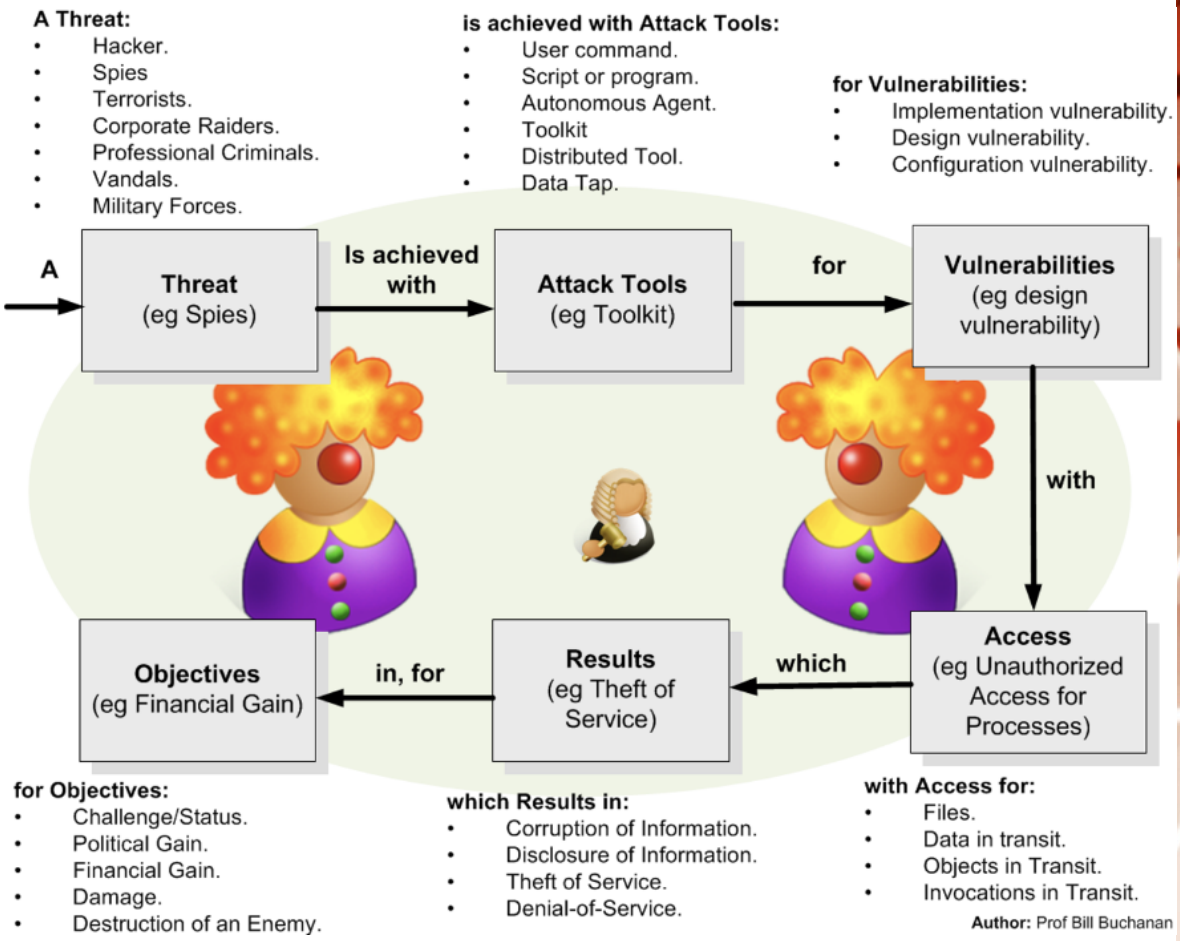


Figure 5

Kill chain model

Within cybersecurity, we see many terms used within military operations, including demilitarized zones (DMZs), defence-in-depth and APT (Advanced Persistent Threat). Another widely used term is the kill chain where military operations would attack a specific target, and then look to destroy it. A defender will then look to break the kill chain and understand how it might be attacked. An example of the kill chain approach is **"F2T2EA", where we Find (a target), Fix (on the location of the target), Track (the movement of the target), Engage (to fix the weapon onto the target), Assess (the damage to the target).** A core of this approach is the provision of intelligence around the finding, tracking and assessment of the target.

Risk | Costs | Benefits & Threat Models

By Team Cygularity

One of the most used cybersecurity models to understand threats is the **kill chain model**, and was first proposed by Lockheed Martin. Yadav et al [2] define that the technical nature of key stages of an attack, include Reconnaissance, Weaponize, Delivery, Exploitation, Installation, and Act on Objective (Figure 6). So let's say that Eve wants to steal the academic records of a university student (Carol). She might perform a reconnaissance activity and find out that Bob is an academic related to Carol's programme of study.

Eve might then determine that Bob runs Windows 10 on his computer, and will then move to weaponization. For this Eve selects a backdoor trojan which fakes the login process for his university site. Eve does this by scrapping the university login system. Next, she picks a suitable delivery mechanism, and decides that a spear phishing method which will trick Bob into logging into the fake Web site. Eve then tries a different phishing email each day and for each attempt, she monitors for any activity of Bob putting in his university login details and his password. Once he is fooled into putting in his username and password, Eve then logs the IP address of his computer, and remotely logs into it. She then installs a backdoor program, and which captures his keystrokes. Eve then monitors his activities, until she sees him logging into the university results system, and where she can capture his login details for this system, and then she can act on her objective and steal Carol's results.

Risk | Costs | Benefits & Threat Models

By Team Cygularity

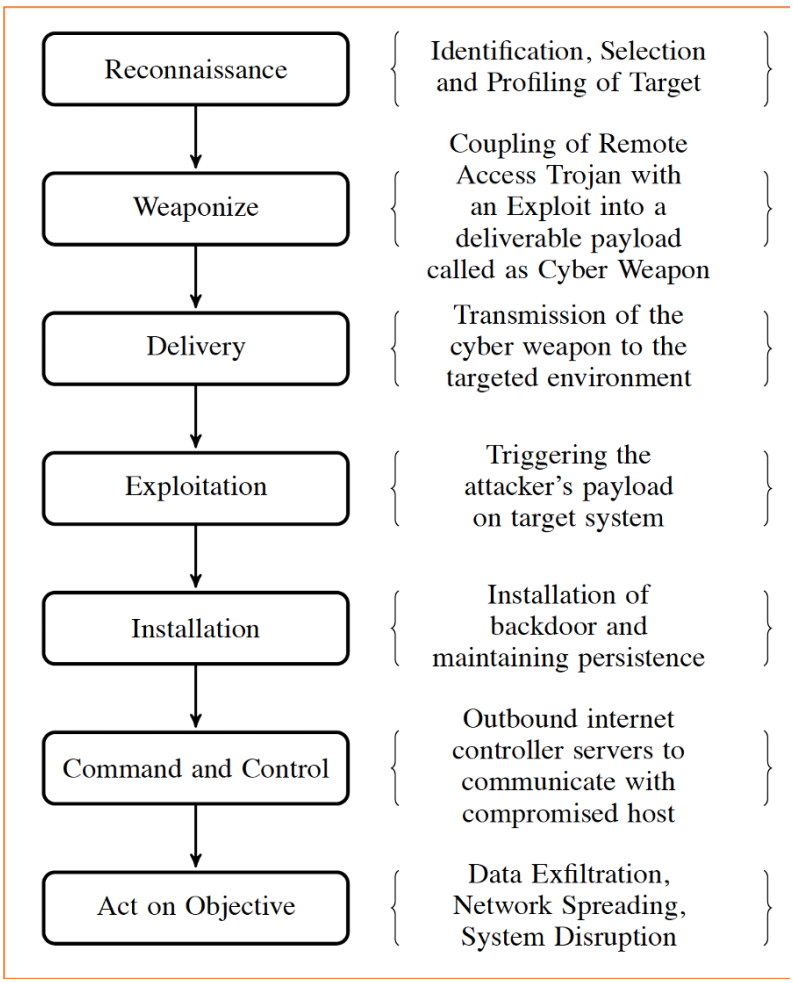


Figure 6 | Cyber Kill Chain(C)

Reconnaissance

The first stages of an attack is likely to involve some form of reconnaissance, and which can either be passive scanning or active scanning. Within active reconnaissance, an attack may use discovery tools to determine servers, networking devices, IP address ranges, and so on. These tools will typically leave a trace on the network, and which could be detected for the reconnaissance activities. Typically an organization would have standard signature detection methods to detect the scanning of IP addresses, TCP ports, and in the discovery of networked services. A company could then black-list, or lock-down, the IP address which sourced the scan.

Risk | Costs | Benefits & Threat Models

By Team Cygularity

With passive scanning an attacker might use open source information to better understand their target. This increasingly involves Open-Source ntelligence (OSINT) Reconnaissance. Increasingly, too, we all leave traces of our activities across the Internet, and as we do, we leak information that could be useful for an attacker. A spear-phishing attack may thus be targeted against a person who has leaked information about their next-of-kin, or on their normal work times. Eve, for example, might know that Carol has a friendship with Trent, and that Carol also uses Pinterest. She then finds out that Carol always starts work at 9am, and that she has been associated with a given IP address. On checking her Twitter account, Eve sees that Carol attended a rock concert the night before. Eve then sends Carol an email just before 9am of:

Hi Carol,
Trent here. Hope you had a great time at the concert. Here are some photos from that I took [here].
— Amit

Eve then sets up a fake Pinterest site, and which asks for Carol's login details. Carol then enters her password, but it is rejected, and then Eve's fake Web page forwards Carol to the correct Pinterest site, and she logs in. Everything looks okay, and Carol just thinks that she has entered the wrong password in the first login attempt. But Eve now sees Carol's username, password and IP address. If Carol uses the same password for many of her accounts, Eve can then move through sites which she is likely to use, and use the Pinterest-sourced password. Thus Eve has used a targeted spear-phishing attack, and where she had determined something about Carol, and then targeted her with something that she thinks Carol will be tricked with.

Risk | Costs | Benefits & Threat Models

By Team Cygularity

Many criticise the kill chain model in cybersecurity as it does not cover all of the possible attacks, and is the limited number in the number of stages. The MITRE ATT&CK(TM) extends these phases into: Initial **Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact,** and the splits these up into techniques used in each phase [3]. Figure 7 outlines that the initial access phase could be achieved those methods such as Drive-by Compromise, and Exploit Public-Facing Application, and which can then be used as a knowledge base for the tactics and techniques used. Within each of the techniques, the framework outlines real-life examples, detection methods, and possible mitigations.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		

Figure 7

MITRE ATTACK

Risk | Costs | Benefits & Threat Models

By Team Cygularity

Peter Polis [4] then brought together the approaches of the kill chain model and the MITRE ATT&CK(TM) knowledge base to created Unified Kill Chain (UKC) model, and which defines 18 unique attack phrases. These are split into stages of an initial foothold and which pivots to network propagation and then with access onto an action (Figure 8). The reconnaissance phases involves: Weaponization; Delivery; Social Engineering; Exploitation; Persistence; Defense Evasion and Command & Control (Figure 9), the network discovery phase involves Discovery; Privilege Escalation; Execution; Credential Access; and Lateral Movement, with an action phrase of Collection; Exfiltration; Target Manipulation; and Objectives.

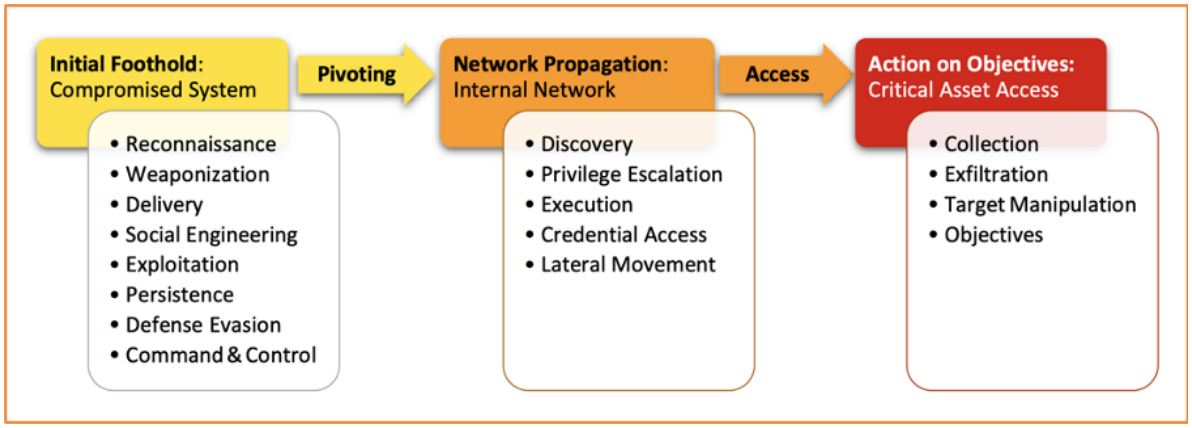


Figure 8

Risk | Costs | Benefits & Threat Models

By Team Cygularity

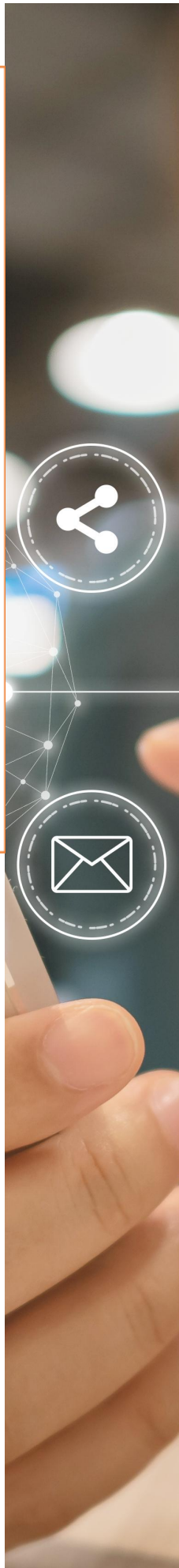
#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Lalibert	Nachreiner	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7	7
8	Command & Control			18		5	7	9	8	8	8	8	8
9	Pivoting					11	13	11	9	9	9	9	9
10	Discovery					14	10	10	11	11	11	10	10
11	Privilege Escalation					17	14	14	10	10	10	11	11
12	Execution					18	12	12	14	14	14	12	12
13	Credential Access						15	13	12	12	12	13	13
14	Lateral Movement						16	17	13	13	13	14	14
15	Collection						8	15	17	17	17	17	15
16	Exfiltration							16	15	15	15	15	16
17	Target Manipulation								16	16	16	16	17
18	Objectives												18

Figure 9

Introducing Cyber Quotient

At the core of cybersecurity are: risks, costs, benefits and threat models. We need common definitions for our definitions, and in defining a common knowledge base. The Unified Kill Chain model goes some way to achieving this.

Regular & Organized RISK ASSESEMENT with common definitions goes a long way in defining the Cyber Security Posture of an Organization.

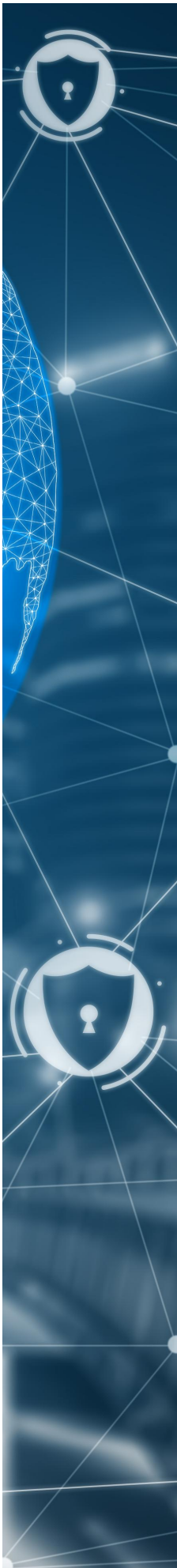


Risk | Costs | Benefits & Threat Models

By Team Cygularity

References

[1] B. Woloch, “New dynamic threats requires new thinking: moving beyond compliance”,” Computer Law & Security Review, vol. 22, no. 2, pp. 150-156, 2006.
[2] T. Yadav and A. M. Rao, Technical aspects of cyber kill chain,” in International Symposium on Security in Computing and Communication. Springer, 2015, pp. 438-452.
[3] MITRE, Mitre’s attack,” 2019. [Online]. Available: https://attack.mitre.org/. Link.
[4] P. Pols, Unifed kill chain (ukc),” 2019. [On-line]. Available: https://www.csacademy.nl/images/scripties/2018/Paul-Pols — -The-Unied-Kill-Chain.
[5] Prof. Bill Buchanan
[6] NIST Framework



cyber quotient
REDEFINING RISK MANAGEMENT

_cygularity
Cyber Security Redefined

Cygularity Sdn Bhd
amitabh@cygularity.com
+60 1111 320221

www.cygularity.com