

# Combating the Cyber-Security Kill Chain: Moving to a Proactive Security Model



**Jim Seaman**

**Abstract** A former boss of mine (Peter Drissell (<https://www.linkedin.com/in/peter-drissell-b917896/>)) (Commandant General RAF Regiment Air Officer Royal Air Force Police) once delivered a presentation at a University lecture, which I had been attending. Here he made the following statement:

Many business leaders regard Security as being very expensive and virtually invisible. That is until it goes wrong, when it becomes very visible and considerably more expensive!

Ever since hearing this statement, I have sought to change this view. Having a proactive, asset and risk focused approach that is aligned with the business mission statements/objectives has a significant impact on changing the business leaders' perspectives. This chapter seeks to explain how you can start to reduce the opportunities for the cyber-attackers, through a more targeted and prioritized approach. Many organizations are feeling a sense of Cyber-security fatigue and often sensing that the cyber-criminals have got the upper hand and that this is a battle that they are losing, frequently believing that they are 'Boiling the Ocean'. If a business fails to identify and categorize their assets, they will not be able to truly appreciate the value of their most important company assets, and their importance to the business. Consequently, when it comes to carrying out the risk assessments, it can often feel like this is based upon a premonition or a hunch. Additionally, when it comes to applying appropriate mitigation controls, this can be extremely difficult to show proportionality and a return on investment.

**Keywords** Asset management · Risk management · Cyber-security · Business stakeholders · Mission statements

---

J. Seaman (✉)  
IS Centurion Consulting Ltd., London, UK  
e-mail: [contact@iscenturion.com](mailto:contact@iscenturion.com)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021  
R. Montasari and H. Jahankhani (eds.), *Artificial Intelligence in Cyber Security: Impact and Implications*, Advanced Sciences and Technologies for Security Applications,  
[https://doi.org/10.1007/978-3-030-88040-8\\_5](https://doi.org/10.1007/978-3-030-88040-8_5)

## 1 Introduction

We are seeing a considerable increase in the number of reported cyber-attacks and organizations that are suffering data breaches. Some of these victims, of the cyber-criminals' activities are not restricted to the small to medium sized businesses and include some large, well-respected, enterprises. This became especially true during the 2020 pandemic, when we observed numerous businesses having to rapidly adjust to new disparate, remote-working business operating models.

However, in most instances it is not the case that the cyber-criminals have started to become increasingly skilled, are using highly sophisticated tactics, techniques & protocols (TTPs) or are employing the very latest tools & technologies.

On the contrary, many of the cyber-criminals are still using some well-established practices to gain unauthorized entry to your corporate environment and valuable assets. Most of today's cyber-criminals are opportunist attackers, seeking to identify the easiest of targets that they can exploit. Although, it is worth noting that there are still those highly organized and well-funded State Sponsored groups, who will have their sights set on undermining the defenses of the better defended high-profile organizations.

Wherever your business resides on the sliding scale of value, there is an enemy out there seeking to target your business and to gain a return on investment (ROI) from your valued assets.

As already mentioned, today's cyber-criminals come in various guises and having varying levels of competence and resources. However, common to all these threat actors are the following three drivers (as depicted in Fig. 1):

Consequently, it is essential that all businesses (*whether large or small*) understand:

– **What assets are important to the continued business operations?**

**Which assets are connected to (*or could impact*) the business critical/important assets?**

- **What are the perceived threats to these assets?**
- **What vulnerabilities are associated with these assets?**
- **If these business critical/important assets become compromised, how much impact will this have on the business?**

To enable this, you need to gain a better understanding of your potential attackers, their 'modus operandi' and how to build a more proactive approach, so that you are more capable at identifying and quickly responding to the stages within the Cybersecurity Kill Chain.

In this chapter, I will describe the foundations of a proactive model, through the application of the **ARMED** acronym:

- **ARMED** (**A**sset & **R**isk **M**anagement for **E**nanced **D**efense).

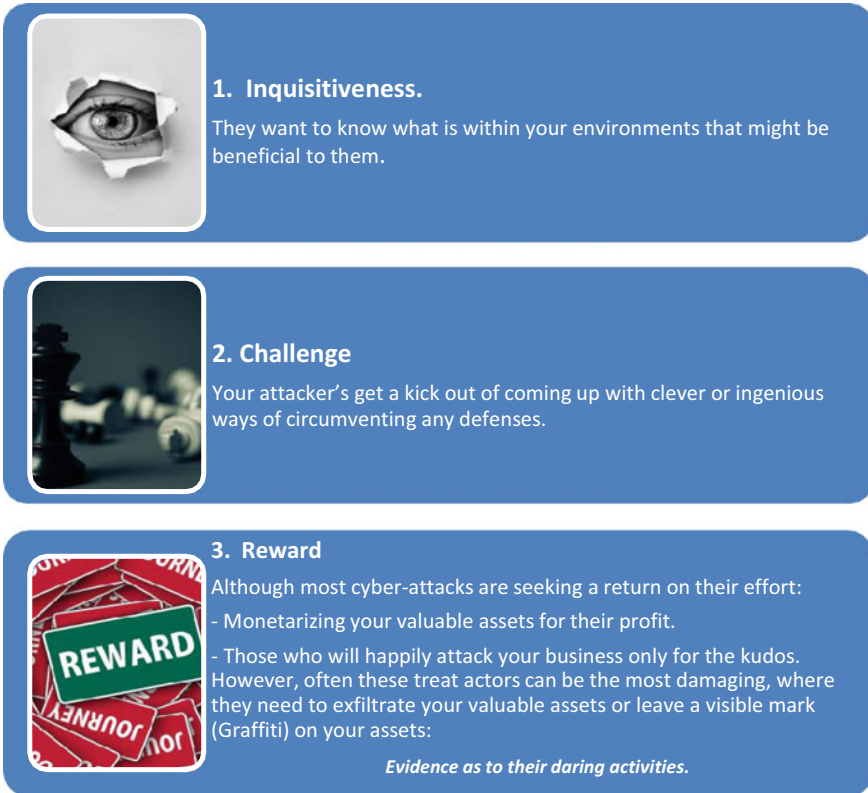


Fig. 1 Cyber attacker drivers

## 2 What is the Cyber Kill Chain?

This term was adapted from the military term ‘Kill Chain’, which was used to describe the stages that an enemy might go through when planning and launching an attack against military establishments and assets.

It became a common place understanding that if you understood the stages that your enemy might go through, then you would be better placed to ensure that your defenses remain effective to quickly identify and respond to any hostile activities. As a result, the defenses would be better placed to contain and limit the potential impact/damage that such attacks could yield.

Throughout military history, there are numerous references to differing variants of the ‘Kill Chain’ model but essentially all identify that any attack goes through various stages:

### F2T2EA [1]

- Find
- Fix
- Track
- Target
- Engage
- Assess.

Later, following the popularity of the internet and the growing number of cyber-attacks, Lockheed Martin adapted the military concept to assist in the defense of cyber-space. They termed this:

### The Cyber Kill Chain [2]

Basically, prefixing the military term with the word ‘Cyber [3]’:

*“word-forming element, ultimately from cybernetics (q.v.). It enjoyed explosive use with the rise of the internet early 1990s. One researcher (Nagel) counted 104 words formed from it by 1994. Cyberpunk (by 1986) and cyberspace (1982) were among the earliest. The OED 2nd edition (1989) has only cybernetics and its related forms, and cybernation “theory, practice, or condition of control by machines” (1962)”.*

In essence, the Cyber Kill Chain model breaks up an attack into the following 7 distinct steps (as depicted in Fig. 2):

Starting with surveillance, the attackers are looking for opportunities they can use to gain an unauthorized persistent presence within their target’s environment. They

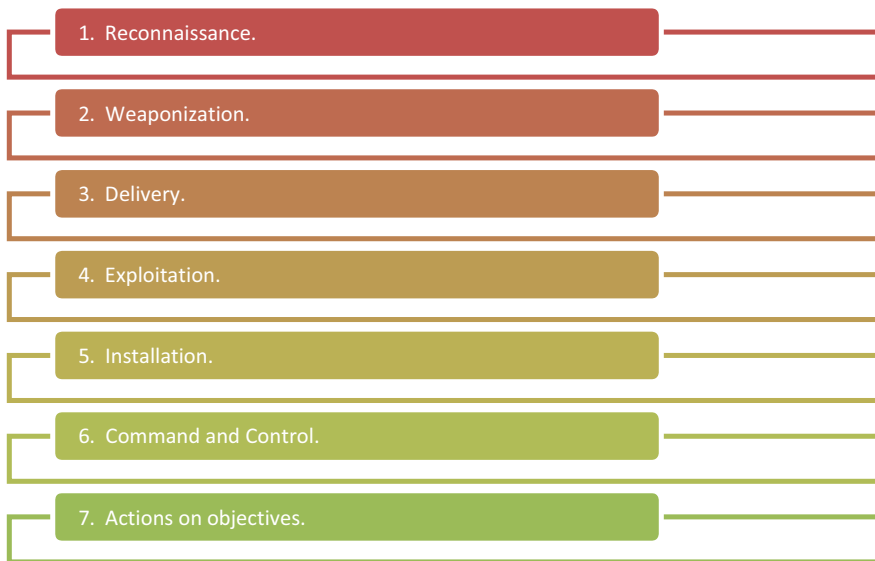
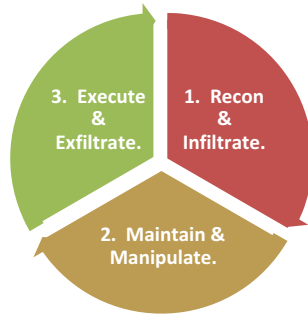


Fig. 2 Cyber kill chain



**Fig. 3** Cognitive attack loop

seek to do this as clandestinely as they can, so that they can achieve the Command and Control that they require to exfiltrate the data or launch the damaging attack.

Much the same as the military version of the term, subsequently, there have been several differing variants of this term:

**Cognitive Attack Loop** [4] (as depicted in Fig. 3).

**Mitre Attack Framework** [5] (as depicted in Fig. 4).

All these models clearly show the fact that the attackers want to understand is what assets you have, where they reside, to categorize the value of these assets and to understand the layout of your environment.

Long before most attackers ‘press the launch button’, will have carried out extensive observations, planning and mapping of their target environment and often having several viable options to choose from.

Most today’s cyber-criminals are in it for the long haul and will patiently play the waiting game, gently tip toeing their way around their target’s infrastructure, often trying not to create too much noise, or testing to see if anyone reacts to a tripped alarm or seeing whether they can cause a distraction to evade being detected.

**Unified Kill Chain** [6].

Building upon the concepts of all the previous versions of the Cyber Kill Chain, the Unified Kill Chain details 18 distinct stages of an attack (as depicted in Fig. 5).

These distinct stages are then aligned with 4 defined phases of an attack path (as depicted in Fig. 6).

However, it is worth noting that in many cyber-attacks, at the point that the organization has detected the presence of an unauthorized entity, they have already gained access (in the **Step 4** phase).

At this point, it is often too late, as this noise being created is the attackers exfiltrating the data and themselves from their victim’s environment.



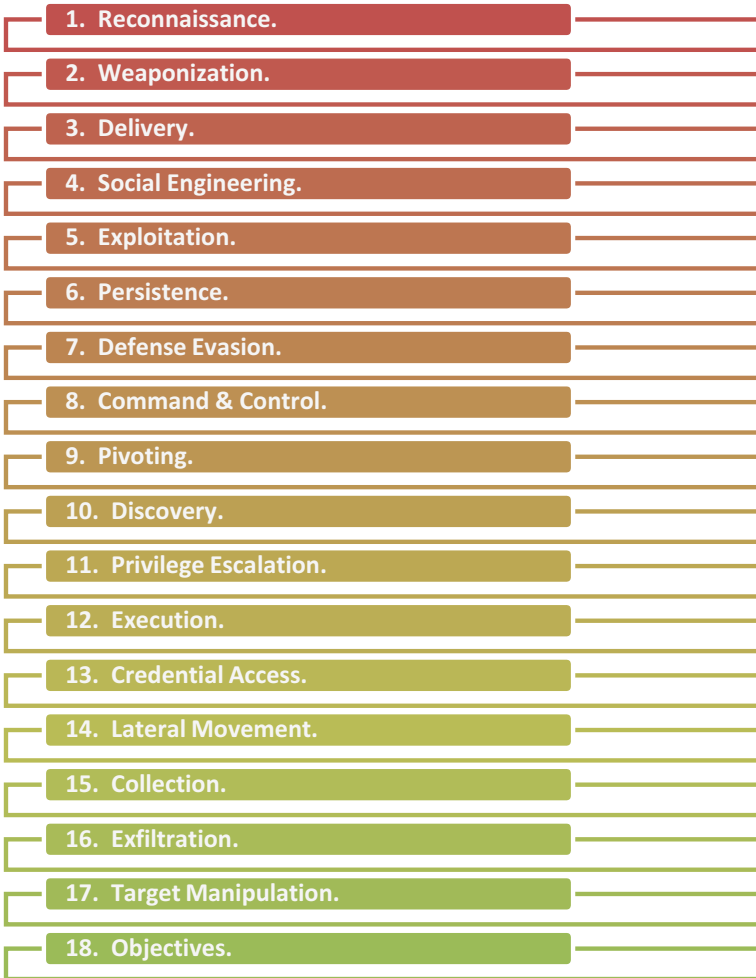
**Fig. 4** Mitre attack framework

*They've grabbed their 'swag' and are hurriedly making their way towards their preplanned exit!*

Consequently, for an effective and proactive defensive model you need to ensure that your defensive efforts can distinguish the **ABNORMAL** activities from the **NORMAL** activities that you would expect from business-as-usual (BAU) operations and be able to quickly recognize the steps from the Cyber Kill Chain, occurring inside your business environment.

### **3 Are You ARMED and Ready?**

An effective and pro-active model needs to apply some of the tactics seen to be employed by your attackers and this starts by fully understanding your environment and knowing what assets present the greatest importance to the business and to have a comprehensive understanding of the potential risks to your business.



**Fig. 5** Unified kill chain

Consequently, for a pro-active approach before considering anything else, you need to understand and manage your assets and risks.

We are learning that the cyber-criminals are starting to embrace machine learning and artificial technologies, to assist them with their cyber-attacks [7], so should we be considering the same with our asset and risk management endeavors?

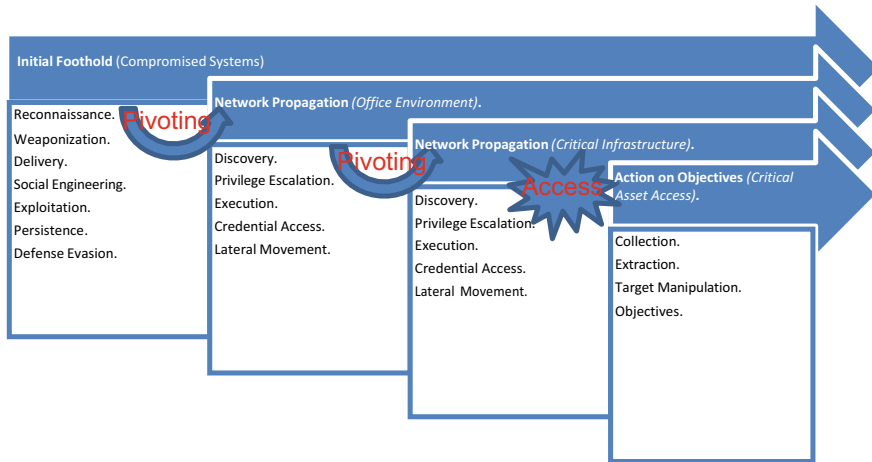


Fig. 6 Attack path

### 3.1 Asset Management

Frequently, many organizations jump straight into compliance modes and forget that their interests should start with engaging with the business' key stakeholders to identify what business operations are the most important to them and to then identify what assets are critical to support these operations?

#### What is an asset?

In a digital and technological age, it is easy for companies to become 'tunnel visioned' into centering on the IT assets. However, it is extremely important to remember that most business processes can be impacted by a compromise of critical non-IT assets.

For instance, look at the impact on businesses (caused by the pandemic) when their personnel were prevented from going into their workplace and they had not established remote working in their business continuity planning.

Or, that organization that has a small number of IT support staff and, as a result, have allowed themselves to have sole employees that are dedicated to delivering specialist operations which only they understand and know how to do. The next thing they know, one of the single points of failure (SPoF) gets seriously ill and is admitted to hospital.

- **Suddenly their SPoF fails and they have no back up.**

Consequently, when defining what an asset is, it is important to ensure that you think far broader than it being just your IT assets.

**NIST Asset Definitions [8]**



- “A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems”.
- “Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards)”.
- “An item of value to achievement of organizational mission/business objectives.

**Note 1:** Assets have interrelated characteristics that include value, criticality, and the degree to which they are relied upon to achieve organizational mission/business objectives. From these characteristics, appropriate protections are to be engineered into solutions employed by the organization.

**Note 2:** An asset may be tangible (e.g., physical item such as hardware, software, firmware, computing platform, network device, or other technology components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, image, or reputation)”.

When considering your assets, you need to look at from a business perspective and identify, and categorize your company operations/processes, based upon their importance to your business mission.

Once you have a priority list of your business operations/processes, you can then start to identify and categorize the assets that support these processes. When considering how to categorize your assets, you should think along the lines of:

- How important are they in support of the continued operation of valuable business processes?
- Are they public facing?
- Are they subject to legal and regulatory obligations (e.g. Financial/Personal data processing).
- Do you have a manual or automated process for detecting those business assets (e.g. IT systems, business applications) that are processing, storing, or transmitting your sensitive data assets?
  - How easily and quickly are you able to locate your sensitive data stores?
- Are they connected to (or able to impact) higher value assets?

For example,

If you have identified a Contact/Call Center as being a valuable and essential part of your business, you will need to break this down into its component parts (as depicted in Fig. 7):

Each of these assets have an importance, in support of the Contact/Call Center operations. However, some are more important than the others and you should



**Fig. 7** Components of a Contact/Call Center

consider maintaining a business asset register, third party supplier register and configuration management database (CMDB), to accurately reflect the assets each valued business operation/process requires.

Additionally, you should also consider creating supporting diagrams to show how the asset dependencies and connections. For example, with a valuable IT asset, connected to the corporate network, you should maintain an accurate network diagram, an example showing the network diagram, for an automatic access control system (AACS), is at Fig. 8. With this, you are better able to easily appreciate and understand the supporting topology, and connectivity.

Where these IT assets have been identified as being essential to the storage, processing or transmission of sensitive business or personal data, you should consider creating and maintaining accurate data flow diagrams (DFD).

Through effective asset management, you should be able to quickly identify any unauthorized, rogue, or dangerous assets that may be attempting to endanger your valued assets or undermine your defensive efforts.

For example.

- A rogue wifi device that is attempting to bypass your firewall.
- A poorly configured unauthorized device, connecting to your corporate network.
- An unauthorized employee attempting to access a restricted area.
- An untethered network connection by a third-party supplier.
- Do you understand the extent of your public-facing digital footprint?

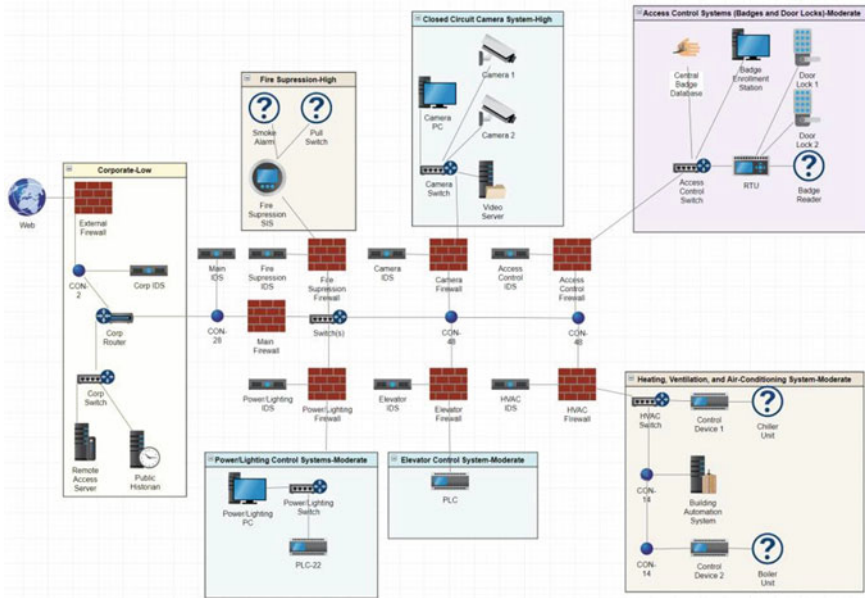


Fig. 8 AACs Network Diagram

– E.g. Monitoring vulnerabilities through a platform such as Security Scorecard [9].

- Can you detect a new public-facing IP, associated with your digital footprint domains?
- Do you understand your different scopes, requiring differing levels of protection?

Where there is electronic monitoring of your assets and their behaviors, automation through Machine-Learning or Artificial Intelligence can really help to enhance your asset management capabilities.

As an example.

- How quickly can you detect someone physically accessing a restricted area, outside their normal working hours, or repeatedly mis-entering their physical access personal identity number (PIN)?
  - Is this a **NORMAL** or an **ABNORMAL** event?
  - Could this be a malicious, accidental, or genuine action?

Both people and business operations tend to become creatures of habit and set routines. Consequently, where you can employ technology to immediately notify you of any activities that are outside your **NORMAL** expected parameters would help enhance your ability to effectively respond to the presence of the **ABNORMAL**.

If you are still struggling to understand what you have in your estate and their criticality or are juggling this through several manual processes, you should consider the benefits that technological solutions can bring to enhance your IT asset management [10], enterprise asset management [11] and access management [12].

**Cyber Security & Infrastructure Security Agency (CISA) Cyber Resilience [13] Asset Management [14].**

If you are looking for a comprehensive guide to asset management, CISA have produced a comprehensive guide, which has been developed to help organizations to establish an effective asset management process.

This guide provides an approach that is common to many asset management standards and guidelines:

1. **Planning for asset management.**
2. **Identifying the assets.**
3. **Documenting the assets.**
4. **Managing the assets.**

Readers of this guide can gain an improved understanding about what an effective the asset management process should involve and to help promote a common understanding of the need for an effective asset management process, including such things as:

- Identifying and describing key practices for asset management.
- Providing examples and guidance to organizations wishing to implement these practices.

### **3.2 Risk Management**

It is only once you have established a proactive approach to understanding the assets within your business environment, can you hope to start to understand what is needed to proportionately safeguard these assets—based upon their perceived value to your business.

All too often, many businesses make the mistake of trying to make everything secure and, as a result, some of the higher-risk (more impactful) assets get overlooked. The reason for this is that there is a distinct difference between the terms ‘Risk’ and ‘Security’.

#### **Risk**

*“1660s, risque, from French risque (16c.), from Italian risco, riscio (modern rischio), from riscare “run into danger,” of uncertain origin. The Englished spelling first recorded 1728. Spanish riesgo and German Risiko are Italian loan-words. With run (v.) from 1660s. Risk aversion is recorded from 1942; risk factor from 1906; risk management from 1963; risk taker from 1892.”*

**Definition [15]**

*“the possibility of something bad happening”.*

### **Security [16]**

*“mid-15c.,*

*“condition of being secure,” from Latin securitas, from securus “free from care” (see secure). Replacing sikerte (early 15c.), from an earlier borrowing from Latin; earlier in the sense “security” was sikerhede (early 13c.); sikernesse (c. 1200).*

*Meaning “something which secures” is from 1580s; “safety of a state, person, etc.” is from 1941. Legal sense of “property in bonds” is from mid-15c.; that of “document held by a creditor” is from 1680s. Phrase security blanket in figurative sense is attested from 1966, in reference to the crib blanket carried by the character Linus in the “Peanuts” comic strip (1956)”.*

### **Definition [17]**

*“protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries”.*

Consequently, before you can apply proportionate protection you need to understand the value of the assets, as well as their associated threats, vulnerabilities and if the assets are compromised, the potential impacts.

- This is the essence of risk management.

Virtually every business cannot operate their business completely securely and they must accept that there will be some risks to their valuable assets. However, the perceived risks must be balanced between proportionality and functionality.

For example

If your business has a small amount of extremely sensitive data records, which need to be proportionately protected to ensure their Confidentiality, Integrity and Availability is maintained, the most robust cause of action might be to (as depicted in Fig. 11):


1. **Put the extremely sensitive data in a waterproof and fireproof safe.**
2. **Lock the safe.**
3. **Destroy the key.**
4. **Dig a hole in the ground.**
5. **Put the safe in the hole.**
6. **Fill the safe with concrete.**
7. **Build a property onto of the concrete.**

However, the reality is that today’s modern businesses are heavily reliant on their data assets and protecting the data in this way may make it more secure but prevents the data from being used in support of business operations.

Consequently, a proactive program needs to look at this using a risk sliding scale, as depicted in Table 1.

**Table 1** Risk sliding scale

UNACCEPTABLE				ACCEPTABLE	
<i>- Sensitive files left in the open</i>	<i>Sensitive files left in the open. In a locked office. 30 min rule</i>	<i>Sensitive files left in the open. In a locked office. In a locked cabinet</i>	<i>Sensitive files left in the open. In a locked office. In a locked safe.</i>	<i>Sensitive files left in the open. In a locked Secure Room. In a locked safe.</i>	<i>Sensitive files left in the open. In a locked Secure Room. In a locked safe. Periodic out of hours security checks.</i>



- The greater the value, the greater the risk=
  - The greater the number of defenses required needed to safeguard the assets, to within acceptable risk levels.

Let’s face it, everyone makes risks decisions every day and this allows you to make and informed decision on the best cause of action that is best for you.

**Think about it:**

**Deciding whether to cross a road** (as shown in Fig. 9):

**Deciding whether to eat that chili pepper (or not)** (as shown in Fig. 10).

With these examples in mind, it is extremely rare that someone would choose their mitigation options without understanding the associated risks. However, it is common place to hear businesses that are applying mitigation security controls when they do not fully understand the value of their assets and the risks that are associated with them.

Consequently, the traditional approach to securing business assets is often seen as providing little of no return on any investments and especially if after all the investments made, the business still feel the impact of a valued asset suffering a compromise of its Confidentiality, Integrity or Availability.

**Threat Modelling**

It is worthwhile understanding the threats that pertain to your valued assets, but what is a threat?

**Threat (n.)** [18]

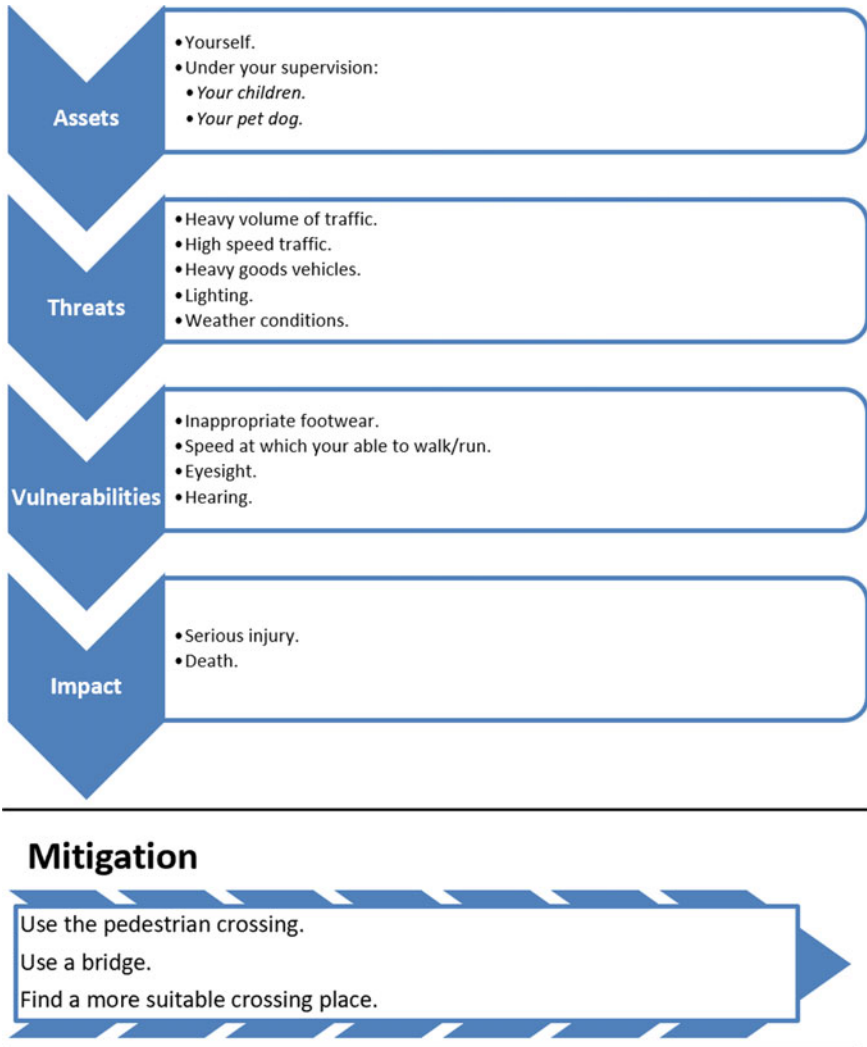
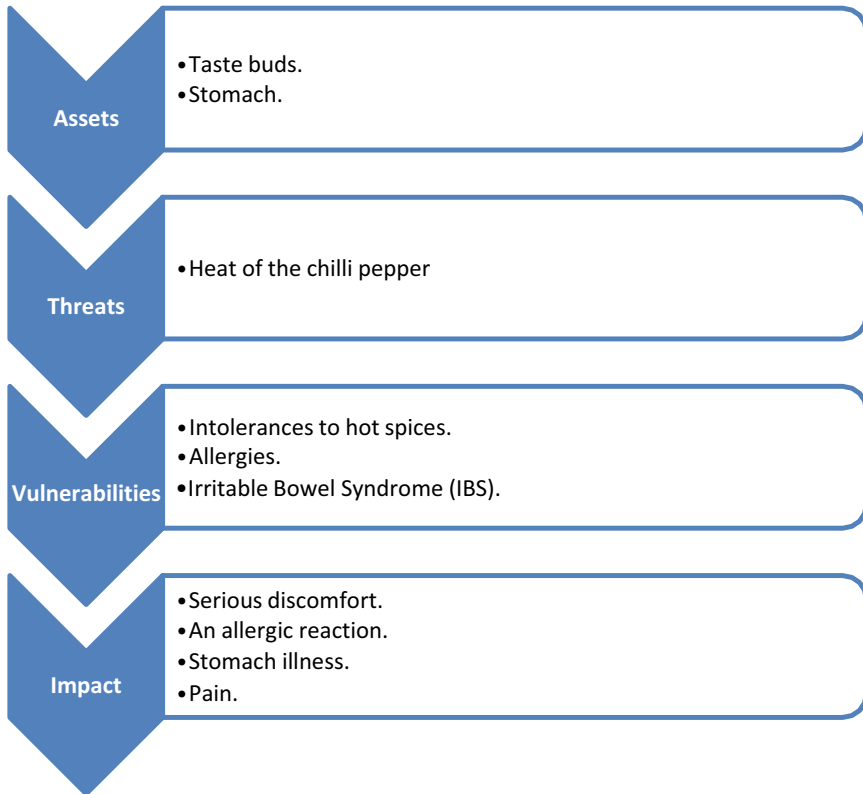


Fig. 9 Road crossing risk assessment

*“Old English preat “crowd, troop,” also “oppression, coercion, menace,” related to preotan “to trouble, weary,” from Proto-Germanic \*thrautam (source also of Dutch verdrieten, German verdrießen “to vex”), from PIE \*treud “to push, press squeeze” (source also of Latin trudere “to press, thrust,” Old Church Slavonic trudu “oppression,” Middle Irish trott “quarrel, conflict,” Middle Welsh cythrud “torture, torment, afflict”). Sense of “conditional declaration of hostile intention” was in Old English”.*



---

## Mitigation

- 
- Have someone else taste it first.
  - Ask for the chilly's heat rating.
  - Have some cold milk at the ready.
  - Choose a lower intensity chili pepper.
  - Choose to avoid eating the chili pepper.

---

**Fig. 10** Chilli eating risk assessment

### Threat Definition [19]

*“In business analysis, Threats are anything that could cause damage to your organization, venture, or product. This could include anything from other companies (who might intrude on your market), to supply shortages (which might prevent you from manufacturing a product).*

*Threats are negative, and external. This mean that threats do not benefit your company, but there is nothing you can do to stop them from coming about.*



*Threats are like opportunities in that you cannot change their frequency, or purposefully bring them about, but you can still choose how to approach them and deal with them”.*

### **NIST Threat Definition [20]**

*“Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.”*

To better understand the threats to your valued assets, you need to have a good appreciation of the threats that might be relevant to these assets. Threats can come in both the traditional and non-tradition types. Traditional threats being best described using the military term TESSOC:

- **Traditional Threats**

Terrorism, Espionage, Sabotage, Subversion and Organized Crime (TESSOC) [21].

- **Non-Traditional Threats**

Theft, Natural Disaster (Pandemic, Fire, Flood, Earthquake, etc.), Investigative Journalist, Hacker, Accident, etc.

To understand how and which of these threats might be relevant for your business, threat modelling becomes immensely helpful.

Threat modeling is a method by which you locate and identify your vulnerabilities, identifying objectives, and then design suitable countermeasures to either prevent or mitigate the effects of cyber-attacks against the system.

To create effective threat models, you should be asking yourself the following types of questions:

- **Which assets are the most valuable and need threat models?**
- **What kind of threat model are required?**

- The answer requires studying network diagrams, data flows, asset inventories/registers, site plans, etc.

*This will help you to create a virtual model of the network you’re trying to protect.*

- **What are the potential problems/issues?**

- Here’s where you discover the main threats to your valued assets.

- **What actions should be taken to recover from a potentially serious incident?**

- You’ve identified some potential problems now; it’s time to work out some actionable resolutions.

- **Was it successful?**

- This step is a follow-up where you conduct a retrospective to monitor the quality, feasibility, planning, and progress.

Basically, you are looking at your business through the eyes of a potential attacker.

- **What would be valuable to your enemies?**
- **What tactics are your enemies known to employ?**
- **Are you vulnerable to such attacks?**
- **Can you see potential opportunities?**

There are many threat models [22] that you can apply, in support of your risk management practices, including:

**Microsoft's STRIDE model [23].**

- ***Spoofing.***

- *Involves illegally accessing and then using another user's authentication information, such as username and password.*

- ***Tampering.***

- *Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.*

- ***Repudiation.***

- *Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. NonRepudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.*

- ***Information Disclosure.***

- *Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.*

- ***Denial of Service.***

- *Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect*

*against certain types of DoS threats simply to improve system availability and reliability.*

- ***Elevation of Privilege.***

- *An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed”.*

### **Process for Attack Simulation and Threat Analysis (PASTA) [24].**

- Define business objectives.
- Define the technical scope of assets and components.
- Application decomposition and identify application controls.
- Threat analysis based on threat intelligence.
- Vulnerability detection.
- Attack enumeration and modeling.
- Risk analysis and development of countermeasures.

### **OCTAVE [25]**

*“Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) is an approach to identify, assess, and manage risks to IT assets.*

*This process identifies the critical components of information security and the threats that could affect their confidentiality, integrity, and availability. This helps them understand what information is at risk and design a protection strategy to reduce or eliminate the risks to IT assets”.*

### **Attack Trees [26].**

*“The tree is a conceptual diagram showing how an asset, or target, could be attacked, consisting of a root node, with leaves and children nodes added in. Child nodes are conditions that must be met to make the direct parent node true. Each node is satisfied only by its direct child nodes.*

*It also has “AND” and “OR” options, which represent alternative steps taken to achieve these goals”.*

### **Vulnerability Modelling**

Having identified and gained a better understanding of the threats that pertain to your valued business assets, you then need to gain a better understanding of the vulnerabilities that are associated with these important business assets, which could be exploited by your threat actors.

**Vulnerability (n.) [27]**

*“1767, noun from vulnerable (q.v.).”*

**Vulnerable (adj.) [28]**

*c. 1600, from Late Latin vulnerabilis “wounding,” from Latin vulnerare “to wound, hurt, injure, maim,” from vulnus (genitive vulneris) “wound,” perhaps related to vellere “pluck, to tear” (see svelte), or from PIE \*wele-nes-, from \*wele (2) “to strike, wound” (see Valhalla).”*

**NIST Vulnerability Definition [29]**

*“Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.”*

In essence, you are looking to identify any exploitable weaknesses that are associated with those assets that need to be adequately protected. Where you have linked assets, you should consider the implications of any vulnerabilities to connected assets, which could be present an aggregated risk.

Each vulnerability should be assessed to ascertain their potential repercussions on your business operations if an opportunist attacker were to take advantage of this weakness.

All vulnerabilities should be identified and prioritized against the safeguarding of the business operations, and remediation road maps maintained to ensure that any high-risk vulnerabilities do not remain beyond the acceptable time scales.

**Impact Modelling**

Just because you have identified some threats and vulnerabilities against your valued business assets, this does not mean that this will present an impact to your business operations, which you need to be concerned about.

**Impact (v) [30]**

*“c. 1600, “press closely into something,” from Latin impactus, past participle of impingere “to push into, drive into, strike against,” from assimilated form of in “into, in, on, upon” (from PIE root \*en “in”) + pangere “to fix, fasten” (from PIE root \*pag “to fasten”). Original sense is preserved in impacted teeth. Sense of “strike forcefully against something” first recorded 1916. Figurative sense of “have a forceful effect on” is from 1935. Related: Impacting”.*

**NIST Impact Definition [31]**

*“With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of*

*information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.”*

However, without an effective business impact analysis (BIA) [32], you will not be able to make an informed choice on whether you are comfortable with the potential impact, or whether you need to reduce the potential impacts to within acceptable levels.

### **3.3 Initial Risk Management**

Before you can start to think about the application of any mitigation controls, you need to understand the level of risks that are inherent to your valued business assets and to what levels of risks your organization’s risk owners are comfortable with. This is termed as identifying the inherent risk and defining the risk appetites:

#### **Initial Risk [33]**

*“Risk before controls or countermeasures have been applied.”*

#### **Risk Appetite [34]**

*“The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.”*

Understanding these terms and how they are applied/implemented in your organization are essential to ensuring that any mitigation efforts remain proportionate to the expectations of the business. You want to ensure that the business is comfortable with the perceived levels of risk and that you’re not applying additional defensive measures than the business needs.

### **3.4 Risk Management Cycle**

There are several risk management frameworks that your organization may choose to baseline against (e.g., NIST Risk Management Framework (RMF) [35]) they all involve several logical steps that should be followed, such as those within the NIST RMF [36], as depicted in Table 2.

However, no matter which specific methodology that a business chooses, most incorporate six key areas of the risk management cycle, as detailed below.

1. **Set strategy.**
2. **Identify risk.**
3. **Prioritize risk.**
4. **Assess mitigation controls.**
5. **Monitor.**

**Table 2** NIST RMF

Prepare	Standards	
1. Categorize System	FIPS 199/SP800-60/CUI Registry	SP800-30
2. Select Controls	FIPS 200/SP800-53/SP800-53B	
3. Implement Controls	Multiple NIST Publications (e.g. SP800-34, SP800-61, SP800-128, etc.)	IR 8062
4. Assess Controls	SP800-53A/IR 8011	
5. Authorize System	SP800-37	SP800-160
6. Monitor Controls	SP800-37/SP800-53A/SP800-137/SP800-137A/IR 8212	SP800-18

## 6. Measure.

### Key objectives

- The strategy for managing risk is set by the board.
- There are distinct processes both to identify and to prioritize risk.
- The existing controls and monitoring procedures are then assessed.
- There is a process to measure the residual risk position and to monitor progress going forward.

Much like running a business, Risk Management should be regarded as a living process, which needs to be subject to dynamic and ongoing management, ensuring that a team effort is applied to help assure that timely identification, assessment, and remediation of risks is maintained.

## 3.5 Risk Assessment

When commencing risk assessments, you need to ensure that you start with the categorization of your efforts so that they align with the business' priorities. You don't want to be focusing your efforts on risk assessing a lower value business process area, ahead of higher value parts of the business.

An effective risk assessment will clearly articulate the perceived levels of risk that the assessed business area is facing and, where these are observed to be above the levels with which the risk owners are comfortable with, you are then better placed to select and suggest appropriate mitigation security controls that can be used to reduce these risk levels, to within acceptable parameters. You should select a range of viable courses of action with which the risk owners can choose from and sign off on.

This decision-making process should be documented, to show governance and that the risk owners were presented the opportunity to make an informed choice as to the best courses of action.

For me, the easiest way to remember and present the course of action options is through the 4 Ts of Risk Management [36]:

- Treat.
- Tolerate.
- Terminate.
- Transfer.

Having successfully identified the potential risks, along with a choice of suitable mitigation solutions, the chosen best course of action needs to be implemented and the risk re-assessed to identify the residual risk and ensure that it has been reduced to within acceptable tolerances.

### **Residual Risk [38]**

*“The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards.”*

## **3.6 Quality Versus Quantity**

Frequently a great deal of businesses either pay lip service to risk management or adopt the simpler risk model of Qualitative risk assessments. However, with risk being so integral and important to the safeguarding of your valued business assets and providing visibility of the return on investment for your risk mitigation, it is beneficial to employ both Qualitative and Quantitative risk assessments.

### **Qualitative Risk**

NIST [39] defines a Qualitative assessment as being:

*“Use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels”.*

Qualitative assessment employs an element of subjective judgment to analyze an organization’s risk based on non-quantifiable information, where individuals are given a reference scale, based upon the organizations risk tolerances. These reference scales are then employed to help with the forecasting of the potential probability and likelihood of the perceived risks, as depicted in Table 3.

These results are then plotted onto a risk heat map (as depicted in Table 4) helping to visualize and scale the risks. However, often this can feel like a ‘finger in the air’ assessment and can be difficult to quantify the potential benefits of any risk mitigation measures.

Consequently, for a comprehensive risk management approach qualitative risk has its place for visualizing risk profiles but these needs to be supplemented by quantitative risk assessments, to help quantify the benefits of any risk mitigation efforts.

### **Quantitative Risk**

NIST [40] defines a Quantitative assessment as being:

**Table 3** Scales of risk

<b>Likelihood (Probability) Value Scales</b>		
<b>Level</b>		<b>Description</b>
<b>Certain</b>	<b>5</b>	<i>Critical likelihood of occurrence. Threat expected monthly.</i>
<b>Likely</b>	<b>4</b>	<i>High likelihood of occurrence. Threat expected on a quarterly basis.</i>
<b>Possible</b>	<b>3</b>	<i>Medium likelihood of occurrence. Threat expected on a 6-monthly basis.</i>
<b>Unlikely</b>	<b>2</b>	<i>Low likelihood of occurrence. Threat is expected annually.</i>
<b>Improbable</b>	<b>1</b>	<i>Extremely low likelihood of occurrence. Threat is seldom to happen (several years).</i>
<b>Impact Value Scales = Average Scale of C. I. A.</b>		
<b>Level</b>		<b>Description</b>
<b>Critical</b>	<b>5</b>	<i>Threats have a critical impact/effect on organization's reputation (e.g. Industrial espionage, accidental or intentional leakage of critical security information to external enemies, etc.).</i>
<b>High</b>	<b>4</b>	<i>Deliberate threats, any occurrence that has a premeditated intent, for example, include a mal-content, important data leakage or modification by an employee, employee unauthorized shredding of important documents, etc. (Unauthorized access, Social engineering).</i>
<b>Medium</b>	<b>3</b>	<i>Accidental threats, any occurrence that doesn't have a premeditated intent, for example, an employee accidentally deleting an important file, failed back-up, etc. (Operational user errors). Natural and Environmental threats (e.g. Earthquake, Lightning, High temperature, etc.)</i>
<b>Low</b>	<b>2</b>	<i>Natural and Environmental threats (e.g. Earthquake, Lightning, High temperature, etc.)</i>
<b>Insignificant</b>	<b>1</b>	<i>Threat source is neither motivated or capable.</i>

***“Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment”.***

With a quantifiable risk assessment, you can see a monetary value of the potential risks and the reduced costs associated to any mitigation efforts. An example, of a quantitative risk assessment is provided at Table 5 [41].

Your risk analysis engagements can be further enhanced through risk analysis with the PESTLE strategic planning model, as depicted in Table 6 [42].

The advantages of PESTLE analysis [43] is that it can prove to be more cost effective, provides a deeper understanding of your business, awareness of the threats, and the potential methods available to exploit opportunities.



**Table 4** Example risk heat matrix

ID	Risk Name					
1	Confidentiality of Information	Likelihood	High	6	3	1
2	Integrity of Information					
3	IT service disruptions, due to poor BCP/DR planning – involving critical systems.					
4	IT service disruptions, due to poor BCP/DR planning – involving non-critical systems.		Medium	8	9	2
5	Fraudulent user activities.					
6	Inadequate change management process.					
7	Security configuration management.		Low	4	7	5
8	Threat Intelligence and Security Event Monitoring.					
9	Vulnerability Management.					
<b>Legend</b>			Low	Medium	High	
		<b>Impact</b>				
<b>Critical</b>	<b>High</b>					
<b>Medium</b>	<b>Low</b>					

## 4 Post Risk Assessment

Having established the importance of having effective asset and risk management processes, it is now essential that any risk assessments can be presented to the appropriate risk owners so that they can make an informed choice on which risk treatment options they think are the most suitable for bringing the risk to within a range in which they are comfortable (Risk Appetite) or deciding whether to escalate to a more senior employee who has been delegated a greater scales of risk appetite.

Each risk decision should be documented and recorded, providing a centralized and hierarchical view of your organization’s risk profile (e.g. Company risk, Geographical risk, Department risk, etc.), as depicted in Fig. 11 [44].

When presenting the risk treatment options, it is extremely important that it is presented in a manner that the Risk Decision Owner can fully understand and appreciate the risks, so that they are able to make an informed decision as to their preferred course of action (CoA).

**Table 5** Quantitative risk assessment

Phishing Risk		Mitigation Measures		
<p><i>The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.</i></p>				
		←	Employ Anti-spoofing controls	
		←	Reduce digital footprint	
		←	Filter/Block incoming emails	
		←	Train users to identify & report suspected phishing emails	
		←	Implement multi-factor authentication (MFA)	
Summary of Simulation Results				
Primary				
		Min	Avg	Max
Loss Events / Year		3	4.16	6
Loss Magnitude		£3.3M	£7.8M	£13.5M
Secondary				
		Min	Avg	Max
Loss Events / Year		1	4.03	6
Loss Magnitude		£3.4M	£4.5M	£6.8M
<b>Vulnerability</b>				<b>99.98%</b>

For example

1. **Define the Problem.**

a. Risk

- (1) Description of the consideration/deduction

2. **Evaluation of Factors**

a. Likelihood

(1) Threat

- i. Description of the consideration/deduction
- ii. Description of the task/constraint

(2) Vulnerabilities

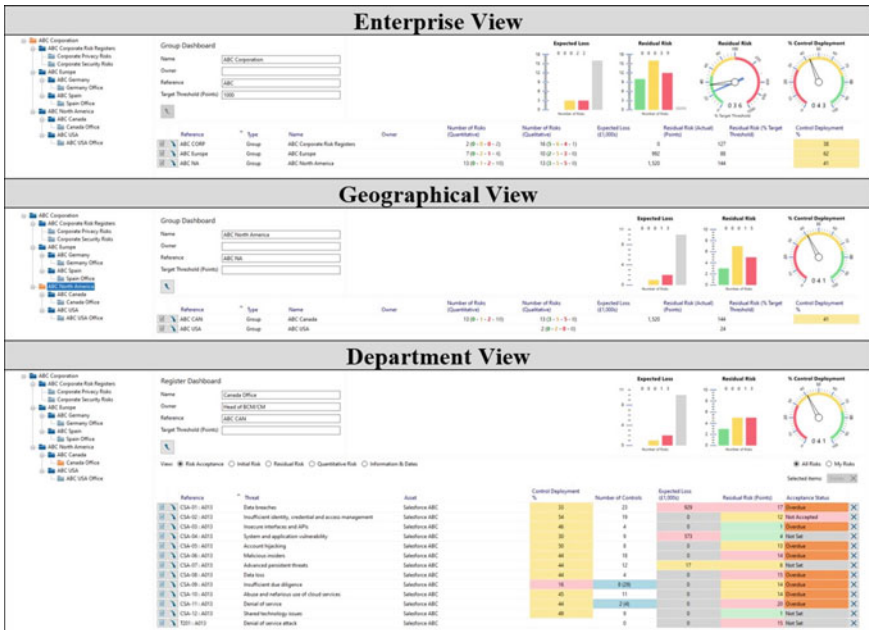
- i. Description of the consideration/deduction
- ii. Description of the task/constraint

(3) Impact

- i. Description of the value
- ii. Description of the output

**Table 6** PESTLE risk analysis

<b>Political</b>	<i>Factors may be altered by the government’s influence on a country’s infrastructure. This may include tax policy, employment laws, environmental regulations, trade restrictions, tariffs, reform and political stability. Charities may need to consider where a government does not want services or goods to be provided.</i>
<b>Economic</b>	<i>Factors include economic growth, interest rates, exchange rates, inflation, wage rates, working hours and cost of living. These factors may have major impacts on how charities operate and make decision.</i>
<b>Social</b>	<i>Factors include cultural aspects, health and safety consciousness, population growth rate and various demographics.</i>
<b>Technological</b>	<i>Factors include ecological and environmental aspects and available products and services. Charities may need to innovate, having considered the compatibility with their own technologies and whether they are transferable internationally.</i>
<b>Legal</b>	<i>Factors include any law which may impact on the charities’ operations, including NGO regulation and criminal and terrorist legislation which will differ from country to country.</i>
<b>Environmental</b>	<i>Factors include an awareness of climate change or seasonal or terrain variations which may affect charities’ service delivery methods.</i>



**Fig. 11** Business risk views

### 3. **Courses of Action (CoA)**

- (1) Intent
  - i. Description of the consideration/deduction
  - ii. Description of the task/constraint
- (2) Commonalities between COAs
- (3) CoA 1
  - i. Description of the consideration/deduction
    - (a) Advantages
    - (b) Disadvantages
  - ii. Description of the task/constraint
- (4) CoA 2
  - i. Description of the consideration/deduction
    - (a) Advantages
    - (b) Disadvantages
  - ii. Description of the task/constraint
- (5) CoA 3
  - i. Description of the consideration/deduction
    - (a) Advantages
    - (b) Disadvantages
  - ii. Description of the task/constraint
- (6) CoA 4
  - i. Description of the consideration/deduction
    - (a) Advantages
    - (b) Disadvantages
  - ii. Description of the task/constraint
- (7) Security Adviser Recommended CoA
  - i. Description of the consideration/deduction
  - ii. Description of the task/constraint

### 4. **Risk Owner's Decision**

- a. Selection of CoA
  - (1) Preferred CoA
- b. Implementation plan
  - (1) Description of how the mitigation controls are to be implemented.
- c. Date of next review
- d. Appointment of Risk Manager.

You can see that this shows a chain of ownership and accountability for the risk decision process, as well as the management of the risk. However, you will also see that in this example, I have provided 4 CoAs. The reason being that if I were to

provide an example with just 3 CoAs, you may fall into the common trap of providing the following CoAs:

1. **The ‘Luxury’ CoA**

- A choice that is comprehensive but completely unproportionate to the perceived value of the asset needing protection.

2. **The ‘Practical’ CoA**

- The preferred choice of the person submitting the risk treatment options.

3. **The ‘Poor’ CoA**

- A completely inadequate or ineffective risk treatment option.

Remember, that all the risk treatment options need to be viable options, so that the risk decisions are made against plausible CoAs and not just tunneling the risk making process into a single option, and the risk owner may even decide to choose not to follow the security advisor’s recommendation.

Having selected the preferred CoA, you should carry out a supplementary risk assessment and document the results. The best way to enhance your proactive security model, is to centralize everything, using an appropriate risk management platform. However, many organizations will struggle on trying to achieve this using the extremely time-consuming and inefficient use of several different spreadsheets and then trying to collate this and provide the various risk views/dashboards that the organization requires.

Consequently, as the proactive security model revolves around effective asset and risk management, you should really be seriously considering putting a suitable software platform at the heart of your proactive security strategy, so that you can instantly gain an appreciation of your asset and risk statuses (as depicted in Fig. 12 [45]).

### **Cyber Security & Infrastructure Security Agency (CISA) Cyber Resilience Risk Management [46]**

If you are seeking to learn more about the Risk Management process, CISA have created an extremely useful and informative guide to help you establish an effective risk management process for your business.

Readers will gain a common understanding of the risk management process and be better placed to identify and describe the key risk management practices, including:

- Identify risks to which the organization is exposed.
- Analyze risks and determine appropriate risk disposition.
- Control risks to reduce probability of occurrence and/or minimize impact.
- Monitor risks and responses to risks and improve the organization’s capabilities for managing current and future risks.

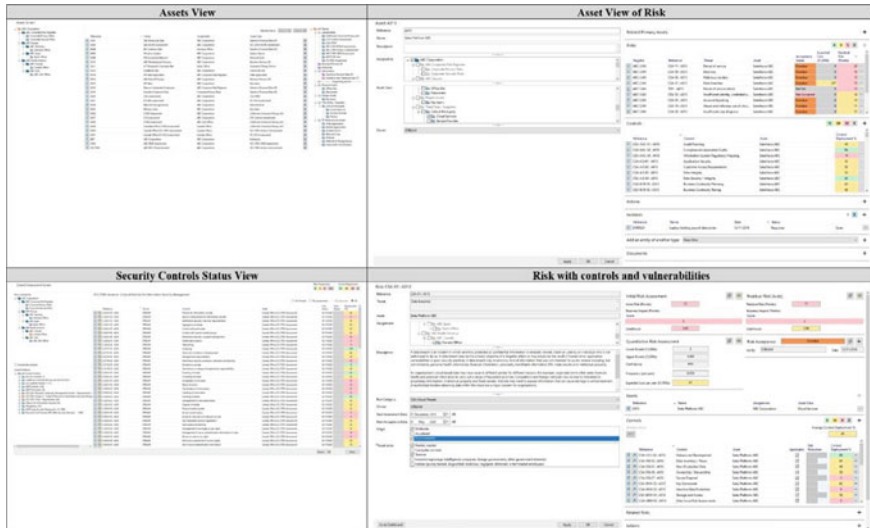


Fig. 12 Assets overview

## 5 Selection of Mitigation Security Controls

Having identified your assets and their associated initial risks, you will then need to select appropriate and proportionate security controls that can be implemented and maintained. When selecting your risk mitigation controls, you can develop your own or select from the numerous industry security resources and controls that are available to business, e.g.,

- **Common Controls** [47].
- **NIST SP800-53 r5: Security and Privacy Controls for Information Systems and Organizations** [48].
- **DoD Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs)** [49].
- **Community Gold Standard** [50].
- **CSA Cloud Controls Matrix (CCM)** [51].
- **ISO/IEC 27,001/2: Information technology—Security techniques—Information security management systems—Requirements** [52].
- **ISO/IEC 27,701:2019: Security techniques—Extension to ISO/IEC 27,001 and ISO/IEC 27,002 for privacy information management—Requirements and guidelines** [53].
- **ISO/IEC CD 27,402: Cybersecurity—IoT security and privacy—Device baseline requirements** [54].
- **PCI DSS** [55].
- **CIS 20 CSCs** [56].
- **ISACA COBIT 2019** [57].

- **Canadian Baseline cyber security controls for small and medium organizations** [58].
- **UK Government Cyber Essentials** [59]
- **CERT Cyber Resilience Maturity Model** [60].
- **OWASP Application Security Verification Standard (ASVS)** [61].
- **OWASP Mobile Application Security Verification Standard (MASVS)** [62].

## 5.1 *Establishing a Security Baseline*

Now, you've established that you have valuable business assets and operations which, if compromised, could impact your organization and that the risks above the levels that you are comfortable with.

Next, you now need to identify the suite of suitable security controls that will provide you with a baseline, with which you are comfortable.

### **Data Privacy Baseline: Call Center Operations**

Your organization has a business unit that provides Call Center operations, and, after the risk assessment, you are far from being happy at the level of risks that this brings to your company. Consequently, you decide to identify some suitable CoAs:

- **Terminate.**

Decide that the risks outweigh the business benefits and decide to disband the Call Center operations, in favor of an alternative business operation.

- **Tolerate.**

Do nothing and hope that these data processing operations are not compromised.

- **Transfer.**

Consider using a third-party service provider to obfuscate the sensitive data, by them converting it into other data formats (e.g. Tokenized Data [63], Dual tone multi-frequency (DTMF) [64], etc.).

- *No longer will your Call Centre IT systems and personnel have a need to interact with any sensitive data assets. However, although the responsibilities have been transferred to the third-party service provider, you still will be accountable for managing that third-party relationship and to ensure that this supplier continues to operate securely, and in line with your expectations.*

- *The questions here are:*

*How great is the risk?*

*How much cost and effort will it take to reduce the risks to a comfortable level, by implementing inhouse security controls?*

*Can the use of outsourced operations enhance the business operations or customer experience?*

*What is the ROI for using the third-party service?*

– Treat.

Reduce the risk by applying the controls from the Common Controls Privacy protection for information and data domain (personal data) and PCI DSS (cardholder data).

By all means consider the added value and assurance of having a cherished business operation or process independently certified against an industry security standard (e.g. ISO/IEC 27001:2013 certification, by an accredited auditor). However, when creating your proactive security model, you should not limit yourself to a single security or compliance framework and ensure that you have a flexible approach that selects the most appropriate security controls (*perhaps chosen from various industry security standards/frameworks*) to help ensure that the perceived risks to your valued business assets remain within your acceptable tolerances.

## 6 Conclusion

Understanding your assets and the risks associated with them should be your number one priority and any strategy should focus on this. Any mitigation security controls should provide a quantifiable benefit in reducing the risks to your organization and not be purely concentrated on an individual compliance or security controls framework.

With asset and risk management being at the heart of an effective proactive security model, you should ensure that your business key stakeholders are provided with a hierarchical and centralized view of the business' valued assets, their associated risks and mitigation security controls status.

The adoption of this proactive approach requires a team effort but will help to harmonize the approach and provide additional visibility and assurance to the key stakeholders, whilst maintaining the risks to within acceptable levels of tolerance. As a result of this approach, the ROI will become more apparent and will improve the understanding that the business benefits that your security strategy is providing.

## References

1. [www.militarydictionary.org](https://www.militarydictionary.org) (n.d.) F2T2EA acronym definition—MilitaryDictionary. <https://www.militarydictionary.org/acronym/m/f2t2ea>. Accessed 10 Feb 2021
2. Lockheed Martin (2019) Cyber Kill Chain®. [online] Lockheed Martin. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.
3. [www.etymonline.com](https://www.etymonline.com) (n.d.) cyber | search online etymology dictionary. <https://www.etymonline.com/search?q=cyber>. Accessed 10 Feb 2021
4. <https://www.carbonblack.com/blog/introducing-the-cognitive-attack-loop-and-its-3-phases/>
5. <https://attack.mitre.org/>



6. Pols P (2017) The unified kill chain designing a unified kill chain for analyzing, comparing and defending against cyber attacks. [https://www.csacademy.nl/images/scripts/2018/Paul\\_Pols\\_-\\_The\\_Unified\\_Kill\\_Chain\\_1.pdf](https://www.csacademy.nl/images/scripts/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf).
7. [www.trendmicro.com](https://www.trendmicro.com) (n.d.) Exploiting AI: how cybercriminals misuse and abuse AI and ML—Security news. <https://www.trendmicro.com/vinfo/hk/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml>. Accessed 10 Feb 2021
8. Editor CC (n.d.) asset(s)—Glossary | CSRC. [online] [csrc.nist.gov](https://csrc.nist.gov/glossary/term/asset). <https://csrc.nist.gov/glossary/term/asset>.
9. [partners.securityscorecard.com](https://partners.securityscorecard.com) (n.d.) Cyber rescue alliance—Member | securityScore-card partner portal partner directory. <https://partners.securityscorecard.com/english/directory/partner/462331/cyber-rescue-alliance>. Accessed 10 Feb 2021
10. Stone M, Irrechukwu C, Perper H, Wynne D, Kauffman L (2018) IT asset management: financial services. <https://csrc.nist.gov/publications/detail/sp/1800-5/final>.
11. Inc G (n.d.) Enterprise asset management (EAM) software reviews 2021 | gartner peer insights. [online] Gartner. <https://www.gartner.com/reviews/market/enterprise-asset-management-software>. Accessed 10 Feb 2021
12. Inc G (n.d.) Network access control (NAC) solutions reviews 2021 | gartner peer In-sights. [online] Gartner. <https://www.gartner.com/reviews/market/network-access-control>. Accessed 10 Feb 2021
13. [us-cert.cisa.gov](https://us-cert.cisa.gov) (n.d.) Assessments: cyber resilience review (CRR) | CISA. <https://us-cert.cisa.gov/resources/assessments>
14. CRR Supplemental Resource Guide Asset Management (n.d.) [https://us-cert.cisa.gov/sites/default/files/c3vp/crr\\_resources\\_guides/CRR\\_Resource\\_Guide-AM.pdf](https://us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-AM.pdf)
15. [Cambridge.org](https://dictionary.cambridge.org) (2019) RISK | meaning in the Cambridge English Dictionary. <https://dictionary.cambridge.org/dictionary/english/risk>
16. [www.etymonline.com](https://www.etymonline.com) (n.d.) Security | origin and meaning of security by Online Etymology Dictionary. [https://www.etymonline.com/word/security#etymonline\\_v\\_30368](https://www.etymonline.com/word/security#etymonline_v_30368). Accessed 10 Feb 2021
17. [Cambridge.org](https://dictionary.cambridge.org) (2019) SECURITY | meaning in the Cambridge English Dictionary. <https://dictionary.cambridge.org/dictionary/english/security>
18. [www.etymonline.com](https://www.etymonline.com) (n.d.) Threat | search online Etymology Dictionary. [https://www.etymonline.com/search?q=threat&ref=searchbar\\_searchhint](https://www.etymonline.com/search?q=threat&ref=searchbar_searchhint). Accessed 10 Feb 2021
19. Frue K (2019) PESTLE analysis—Business and SWOT analysis. [online] PESTLE analysis. <https://pestleanalysis.com>
20. [Nist.gov](https://csrc.nist.gov) (2015) Threat—Glossary | CSRC. <https://csrc.nist.gov/glossary/term/threat>
21. Royal Navy MOD UK (2017) CHAPTER 29 ESTABLISHMENT/UNIT SECURITY OFFICER. Duties of the Establishment/Unit Security Officer. Accessed 10 Feb 2021
22. Exabeam (2020) 6 threat modeling methodologies: prioritize & mitigate threats. <https://www.exabeam.com/information-security/threat-modeling>. Accessed 10 Feb 2021
23. jegeib (n.d.) Threats—Microsoft threat modeling tool—Azure. [online] [docs.microsoft.com](https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats). <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats>
24. Reliable Cyber Solutions (2020) PASTA threat modeling method: all you need to know—RCyberSolutions.com. <https://www.rcybersolutions.com/pasta-threat-modeling-method-all-you-need-to-know>. Accessed 10 Feb 2021
25. EC-Council (n.d.) Threat modeling | importance of threat modeling. <https://www.eccouncil.org/threat-modeling>. Accessed 10 Feb 2021
26. [Simplilearn.com](https://www.simplilearn.com) (2020) What is threat modeling: process and methodologies. <https://www.simplilearn.com/what-is-threat-modeling-article>
27. [www.etymonline.com](https://www.etymonline.com) (n.d.) vulnerability | search online etymology dictionary. [https://www.etymonline.com/search?q=vulnerability&ref=searchbar\\_searchhint](https://www.etymonline.com/search?q=vulnerability&ref=searchbar_searchhint). Accessed 10 Feb 2021
28. [www.etymonline.com](https://www.etymonline.com) (n.d.) vulnerable | origin and meaning of vulnerable by online etymology dictionary. <https://www.etymonline.com/word/vulnerable>. Accessed 10 Feb 2021
29. [Nist.gov](https://csrc.nist.gov) (2015) vulnerability—Glossary | CSRC. <https://csrc.nist.gov/glossary/term/vulnerability>

30. [www.etymonline.com](https://www.etymonline.com) (n.d.) impact | origin and meaning of impact by online etymology dictionary. [https://www.etymonline.com/word/impact#etymonline\\_v\\_1545](https://www.etymonline.com/word/impact#etymonline_v_1545). Accessed 10 Feb 2021
31. Editor CC (n.d.) Impact—Glossary | CSRC. [online] [csrc.nist.gov](https://csrc.nist.gov). <https://csrc.nist.gov/glossary/term/impact>. Accessed 10 Feb 2021
32. Excel TMP (2016) Business impact analysis template excel. <https://exceltmp.com/business-impact-analysis-template-excel>. Accessed 10 Feb 2021
33. IADC Lexicon (2017) Definition of initial risk. <https://www.iadclexicon.org/initial-risk>. Accessed 10 Feb 2021
34. Editor CC (n.d.) Risk appetite—Glossary | CSRC. [online] [csrc.nist.gov](https://csrc.nist.gov). [https://csrc.nist.gov/glossary/term/Risk\\_Appetite](https://csrc.nist.gov/glossary/term/Risk_Appetite). Accessed 10 Feb 2021
35. nicole.keller@nist.gov (2020) Risk management framework. [online] NIST. <https://www.nist.gov/cyberframework/risk-management-framework>
36. Blank R, Gallagher P (2012) Guide for conducting risk assessments NIST special publication 800–30 Revision 1 JOINT TASK FORCE TRANSFORMATION INITIATIVE. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>
37. Giles S (2012) Managing fraud risk : a practical guide for directors and managers. Wiley, Chichester, West Sussex
38. Editor CC (n.d.) Residual risk—Glossary | CSRC. [online] [csrc.nist.gov](https://csrc.nist.gov). [https://csrc.nist.gov/glossary/term/residual\\_risk](https://csrc.nist.gov/glossary/term/residual_risk). Accessed 10 Feb 2021
39. Editor CC (n.d.) Qualitative assessment—Glossary | CSRC. [online] [csrc.nist.gov](https://csrc.nist.gov). [https://csrc.nist.gov/glossary/term/Qualitative\\_Assessment](https://csrc.nist.gov/glossary/term/Qualitative_Assessment). Accessed 10 Feb 2021.
40. Editor CC (n.d.) Quantitative assessment—Glossary | CSRC. [online] [csrc.nist.gov](https://csrc.nist.gov). [https://csrc.nist.gov/glossary/term/Quantitative\\_Assessment](https://csrc.nist.gov/glossary/term/Quantitative_Assessment). Accessed 10 Feb 2021
41. [app.fairu.net](https://app.fairu.net) (n.d.) FAIR-U. <https://app.fairu.net>. Accessed 10 Feb 2021
42. Tool 3: Risk management (n.d.). [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/550691/Tool\\_3.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550691/Tool_3.pdf)
43. Bush T (n.d.) 3 tools to include in risk management framework for best results. [online] [pestleanalysis.com](https://pestleanalysis.com). <https://pestleanalysis.com/risk-management>. Accessed 10 Feb 2021
44. Acuity Risk Management (n.d.) STREAM integrated risk management software. <https://acuityrm.com>. Accessed 10 Feb 2021
45. Acuity Risk Management (n.d.) STREAM, cyber risk & compliance management platform. <https://acuityrm.com/platform>. Accessed 10 Feb 2021
46. CRR Supplemental Resource Guide Risk Management (n.d.). [https://us-cert.cisa.gov/sites/default/files/c3vp/crr\\_resources\\_guides/CRR\\_Resource\\_Guide-RM.pdf](https://us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-RM.pdf). Accessed 10 Feb 2021
47. Common Controls Hub (n.d.) Compliance mapping for PCI, HIPAA, and more. <https://commoncontrolshub.com>. Accessed 10 Feb 2021
48. NIST (2020) Security and privacy controls for information systems and organizations. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
49. [public.cyber.mil](https://public.cyber.mil) (n.d.) Security technical implementation guides (STIGs)—DoD cyber exchange. <https://public.cyber.mil/stigs>. Accessed 10 Feb 2021
50. [public.cyber.mil](https://public.cyber.mil) (n.d.) Community gold standard (CGS)—DoD cyber exchange. <https://public.cyber.mil/cgs>. Accessed 10 Feb 2021
51. Cloud Security Alliance (n.d.) Cloud security alliance. <https://cloudsecurityalliance.org/research/cloud-controls-matrix>. Accessed 10 Feb 2021
52. ISO—International Organization for Standardization (2019) ISO/IEC 27001:2013. [online] ISO. <https://www.iso.org/standard/54534.html>.
53. 14:00–17:00 (n.d.) ISO/IEC 27701:2019. <https://www.iso.org/standard/71670.html>. Accessed 10 Feb 2021
54. 14:00–17:00 (n.d.) ISO/IEC CD 27402. [online] ISO. <https://www.iso.org/standard/80136.html>. Accessed 10 Feb 2021
55. [Pcisecuritystandards.org](https://www.pcisecuritystandards.org) (2019) Official PCI security standards council site—Verify PCI compliance, download data security and credit card security standards. <https://www.pcisecuritystandards.org>

56. CIS (2018) The 20 CIS controls & resources. <https://www.cisecurity.org/controls/cis-controls-list>
57. Isaca (2019) COBIT | control objectives for information technologies | ISACA. [online] Isaca.org. <https://www.isaca.org/resources/cobit>
58. BASELINE CYBER SECURITY CONTROLS FOR SMALL AND MEDIUM ORGANIZATIONS FOR SMALL AND MEDIUM ORGANIZATIONS. (n.d.) <https://cyber.gc.ca/sites/default/files/publications/Baseline%20Cyber%20Security%20Controls%20for%20Small%20and%20Medium%20Organizations.pdf>. Accessed 10 Feb 2021
59. [www.ncsc.gov.uk](https://www.ncsc.gov.uk) (n.d.) About cyber essentials. <https://www.ncsc.gov.uk/cyberessentials/overview>
60. [us-cert.cisa.gov](https://us-cert.cisa.gov) (n.d.) Assessments: cyber resilience review (CRR) | CISA. <https://us-cert.cisa.gov/resources/assessments>. Accessed 10 Feb 2021
61. [owasp.org](https://owasp.org) (n.d.) OWASP application security verification standard. <https://owasp.org/www-project-application-security-verification-standard>
62. [owasp.org](https://owasp.org) (n.d.) OWASP mobile security testing guide. <https://owasp.org/www-project-mobile-security-testing-guide>
63. Zortrex (n.d.) Data protection—Secure tokenisation solutions. [online] Zortrex. <https://www.zortrex.com>. Accessed 10 Feb 2021
64. [www.gccicom.net](https://www.gccicom.net) (n.d.) Gartner recognised contact centre solutions from GCI. <https://www.gccicom.net/Our-Services/Unified-Communications/GCI-Contact-Centre>. Accessed 10 Feb 2021