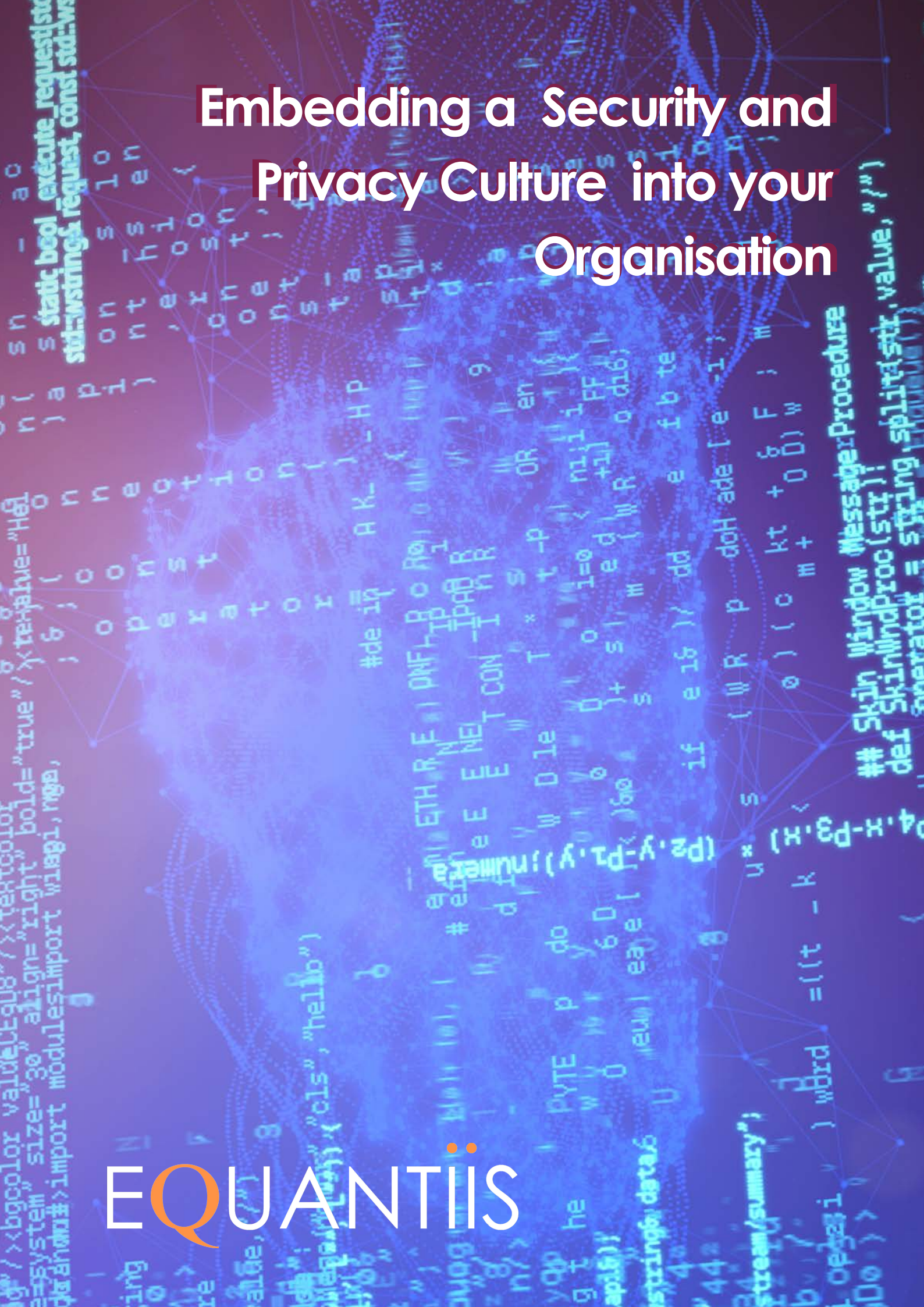
Embedding a Security and Privacy Culture into your Organisation



EQUANTIIS

Introduction

Since the introduction of GDPR, the words 'data breach' and the associated fears have begun to trickle into the lexicon of staff at all levels across an organisation. Whilst this has pushed the concept of privacy, and to an extent internal data security, to the forefront, it hasn't necessarily been adopted into an organisation's culture.

For the majority of organisations, GDPR implementation has been a compliance exercise, led by Legal and left to IT to undertake any changes to generic systems and those that Marketing or Sales use (possibly with vender support). It would have been considered a technology problem and focus would be placed on the teams that would invoke the most risk of a data breach as they use the most data day to day. Now that launch plans have passed and policies have been drafted, are they understood, and have they been adopted?

But, what of security? There's no denying that GDPR has been a great catalyst for improving security processes within an organisation, but unless an organisation is regulated by the Financial Conduct Authority (FCA), or is part of the critical national infrastructure which requires compliance with additional frameworks (EU Directive on the security of Network and Information Systems) then security work may have been limited to protecting data under GDPR.

It was reported that over four in ten businesses and two in ten charities experienced a cyber security breach in 2018. Like GDPR, it is also highly possible addressing the problem remains largely fragmented, with Facilities Management handling the physical security, Cyber Security managed by IT, and website security potentially handled by Marketing and suppliers reactively.

If organisations do not consider the possible threats and how they approach mitigation as ONE organisation, then they are at risk of not only data loss but potential financial and reputational damage.

If, as Robert Mueller (former Director of the FBI) said "there are only two types of companies: those that have been hacked and those that will be!", how can organisations pivot from those that do not embed a privacy and security culture, to those that do?

Contents

Understanding what you are protecting, and its associated risks	4
Evaluate your organisation by baselining and then benchmarking	6
Demonstrating Value of Investment in Cyber Security	8
Defining a Mitigation Based Strategy	9
People, People, People - Changing the Mindset from Technology to Management	10
Conclusions	12

Understand what you are protecting, and its associated risks

The most effective starting point is to understand what an organisation needs to protect. What are its primary assets (its Crown Jewels!), and who has internal responsibility?

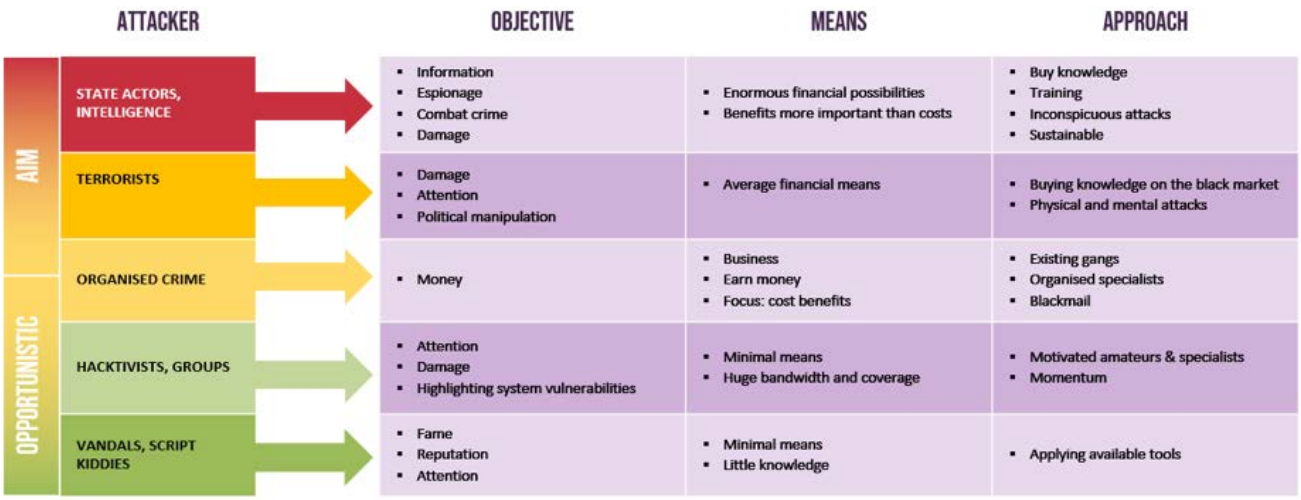
This may include - but is not limited to:

- Data
- Money
- Intellectual Property
- Critical Infrastructure
- Reputation

Whilst typically in Equantiis' experience, the most common causes of breaches are:

- Negligence (lost data, devices and keys);
- Malicious or criminal attacks (hacking or theft of electronic devices);
- Corporate espionage/ex-employees with a grudge.

Understanding what you are protecting will also give an insight into the type of Cyber Criminal that may target you, their objectives, means and approach.



Once you have identified what you need to protect, and from whom, then you can begin to understand your current threat level.

If you have already started this conversation internally then you may have already begun considering how to approach cyber security within your organisation, if not then you should begin immediately.

For many organisations, this workstream will likely be sponsored by a Chief Financial Officer, Chief Information Officer, or Chief Technical Officer. Typically, the same people who would manage organisational risk.

In sectors such as engineering, understanding the risk landscape and the associated mitigations is the purview of the project manager who produces and regularly maintains a 'risk register'.

A risk register is a repository for all risks identified and includes additional information about each risk, e.g. nature of the risk, reference and owner, mitigation measures. This methodical approach to risk management is considered a flagship means of identifying risks, understanding the potential impact and putting in place mitigations where required.

Companies of all sizes often employ similar risk management approaches to better understand organisational risks that they may face. These 'risk registers' are usually owned and managed at board level.

As discussed above, the detailed risks posed by cyber security are often seen as a compliance exercise and dealt with by Compliance Managers or the IT department. Many organisations may not therefore fully recognise the risks and actively mitigate the threats posed by a breach at board level. A security incident can trigger a domino effect within an organisation.

Evaluate your Organisation by baselining and then benchmarking

A baselining exercise will help you establish where the company is in relation to security and privacy strategy and then help point out areas to focus on. This would typically include, but is not limited to;

- Policy
- Staff
- Physical security
- Technology (including infrastructure and systems)
- Workplace setting
- Data

The main objective of the baseline exercise is objectivity/transparency. Without objectively baselining your organisation, you cannot effectively plan the way forward and clearly identify the barriers to progress. Since GDPR is over a year old some of this discovery may have already been completed in your organisation, and a project team may even have previously existed that would have some of this domain knowledge.

It is also useful to assess how your organisation fares against its peers to understand whether shared challenges exist. There is a tendency for organisations to think they are unique, but there is also a lot to learn from other sectors that may approach things differently.

This exercise will show where you have coverage, and it may be apparent where some gaps exist. This is the perfect time to begin to think about the people element as the baseline will act as a litmus test of the organisation's culture with regards to its understanding of security and privacy issues.

You will also have identified the current spend and which internal cost centres have control of the expenditure. It is recommended to develop a single cost centre for security that provides a focus and authority in a specific environment. This may then enable the mobilisation of an internal team that can commence conversations and gain an understanding about where investment is being made; and where it should be made.

What is the right level of investment for cyber security mitigations by an organisation? There is no simple answer as it is a loaded question, but at a high level it will depend on how the organisation functions and its overall risk appetite. As a minimum, organisations should be able to demonstrate that they comply with GDPR and ensure they are actively doing what they need to protect the data of their customers, staff, and its primary assets. A rounded organisation approach which considers both people and technology is a strong defence.

Everything has a value, and data is no exception. The phrase 'data is the new oil' is quite often used when referring to data and its value. Understanding the value of your customer's data is considered key to determining how much an organisation should invest in cyber security mitigations.

What if you believe that more investment is required, how do you convince your board to make an appropriate level of investment?

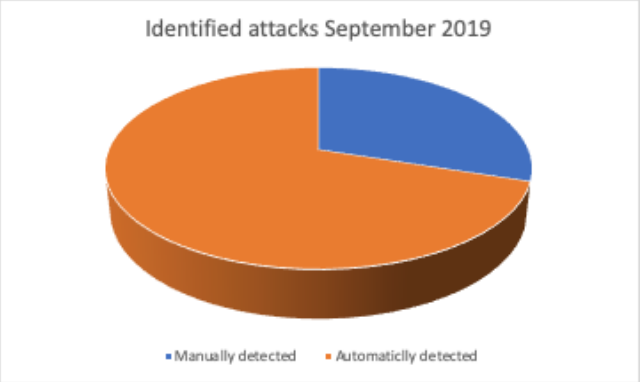
Demonstrating the Value of Investment in Cyber Security

Part of the challenge of securing the investment at board level is the difficulty in demonstrating a Return on Investment (ROI) for cyber security. Without this capability, organisations address cyber investment through compliance channels, which limits the organisations ability to proactively mitigate threats.

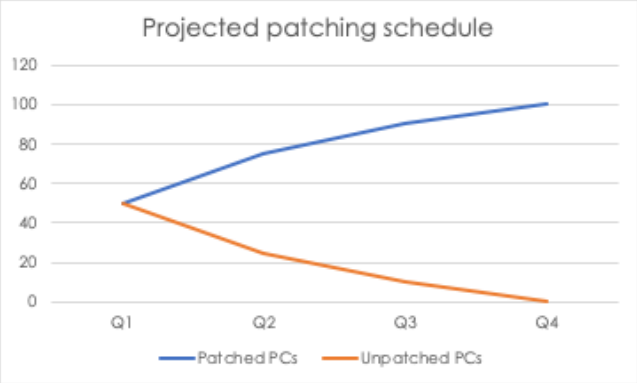
Put simply, cyber investment via compliance ensures your organisation does not incur any fines. Cyber investment through a risk management lens, allows your organisation to invest as much (or as little) as you want to protect against threats to your key assets.

The use of risk management tools provides a framework in which the organisation can correlate investment and risk to assets, a language familiar to a board.

Using 'technical' jargon and statistics are not helpful as decision makers may not understand the real issues but translating these into lay persons terms will offer benefit. For example, a table outlining details of the number of SQL injections discovered in a month would not hold as much value as a chart highlighting 'number of attacks' broken down by 'automatically' and 'manually' detected.



Using 'duration' as a metric to project the completion of a task also visualises risk. This example highlights the time to patch all of an organisation's machines.



Sharing the level of staff awareness is also key and gives a baseline for improvement.

All of these examples help illustrate a need for improving either process, technology or staff awareness.

Defining a Mitigation Based Strategy

Understanding the cyber security risks and the potential impact allows organisations to consider the mitigations that may need to be put in place. The risk management framework allows organisations to better understand the true risk landscape, and the potential impact of each individual risk. The organisations are then in a position where they can assess each risk and decide how they want to deal with it. There are four ways in which they can usually proceed:

- Avoid. These are risks that can be bypassed and will no longer have an impact on the organisation.

- Reduce. This is where the impact of a risk is reduced by investment that either reduces its impact or its probability of occurrence to a value that is more acceptable to the organisation.

- Transfer. Pass the risk over to another party, i.e. to a third party, such as a supplier, or insure against the risk. This does not change or eliminate the risk but changes the risk owner.

- Accept. There are risks that are often not worth investing to mitigate against, i.e. costs outweigh benefits. In these cases, the organisation accepts the risks. The decision on accepting risks is decided by the risk appetite of an organisation.

It should be noted that it not possible to completely eliminate all risks, i.e. risks will always exist. It is also usually accepted that you cannot identify all risks. To get the best coverage, organisations need to get all key stakeholders with understanding of the issue involved in the risk identification and management process. It is also important to refresh the risk register regularly to ensure new risks are captured and brought to the attention of the key decision makers, especially if there may be a material impact on the business.

People, People, People - Changing the Mindset from Technology to Management.

Security and privacy are to a greater extent a management issue and not a technology issue. Systems and infrastructure are managed or configured by humans, and users of such would typically follow processes to utilise them. When shortcuts are taken and processes aren't followed, this begins to introduce potential for error and risk. Organisations are typically good at preparing policies to meet regulatory requirements but less successful at implementing plans to disseminate and raise awareness in the workforce.

Solutions are not primarily geared towards a large investment into high-end hardware and software. Although investment in a solution is needed, putting emphasis on mitigations against the impact people may have should be the number one priority of organisations; as this is the most common theme behind most cyber security breaches.

Although frequently overlooked, improving staff understanding of cyber-risks through training and other forms of raising awareness can have a significant impact on reducing the probability of risks from occurring, and is often a very low cost investment to achieve.

Areas such as the Defence and Construction Sectors have been hugely successful in implementing effective policies, processes and plans to enforce good behaviours and incorporate lessons learnt to improve further. The companies in these sectors are performing activities that have high stakes, and complacency could have significant repercussions to an organisation. Some potential examples are:

1. Loss of data or intellectual property (IP) in areas of defence could impact National Security;
2. Breaches to critical infrastructure could have a significant impact on the day to day functions of citizens;
3. Lax safety culture in the Construction Industry could result in incidents that may have a detrimental impact on company reputation, cause injury / fatalities, loss of future business and even regulatory prosecution and fines.

The three examples above can be related to cyber security risks. The loss of IP in the areas of defence could just as easily be the sole revenue stream for a business that may lose significant investment as a result.

The WannaCry attack on the NHS in 2017 is a typical example where critical national infrastructure was put at risk due to a cyber breach. A lax safety culture could be assimilated as a lax implementation of cyber prevention mechanisms, which can have a detrimental impact on a company's reputation, affect your employees and customers and cause loss of future revenue.

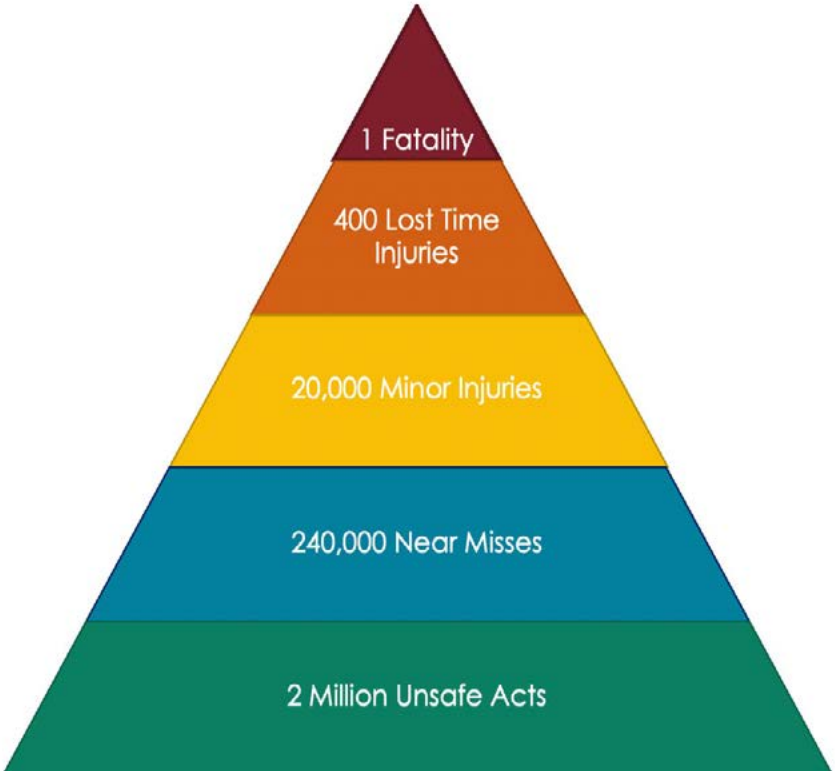
Organisations that have put in measures that focus on the small actions and disseminate the importance across all employees have successfully changed the overall mindset of its staff. A good example of this is the act of holding the hand rail whilst using the stairs.

In the Oil and Gas Sector, the messaging is applied equally in the office as it is on a site, as an employee can cause an accident anywhere.

Meet any worker from that sector, you will find that this behaviour is ingrained in their DNA and they will hold the handrails wherever they walk.

This can be further generalised to the way in which the Engineering Sector approaches safety. The mindset of its employees has been tuned in a way so that everyone is always vigilant and on the look-out for potential hazards. Simple reporting mechanisms are set-up that allow employees to report incidents, including potential incidents such as near misses and unsafe behaviours.

The Heinrich's Triangle below is often used to record and present the data.



Conclusions

Cyber Crime is a growing challenge facing organisations of all sizes. Even before the implementation of GDPR, many sectors successfully implemented measures to help people within their organisation adapt a vigilant and a questioning attitude. These exemplars have begun to develop a culture and mindset in people of continual awareness, which improves as the threat landscape shifts.

For organisations that are beginning this journey there are lots of takeaways for other sectors to learn from to build a strong security posture.

Always start with the 'what', 'who', 'where', 'how', and 'why' and bring the whole organisation along with you, by finding ways to communicate with them that limits jargon, demonstrates a return on investment and ensures measurement is in place.

Changing culture and internal mindset is something that all organisations should aspire to when it comes to enhancing the security posture. With the rising threat that is evolving daily, it is the responsibility of all employees to be vigilant and to be responsible both in the professional and personal world.

Author

Nick David
nick.david@equantiis.com

Contact Us

hello@equantiis.com

@equantiis

020 3376 7447

EQUANTIIS