Тетяна Венкель

Методична розробка з аналітичного фахового читання англійською мовою

до монографії: "Кібербезпека для початківців"

"CYBERSECURITY FOR BEGINNERS"

Raef Meeuwisse, Icutrain Ltd, 37 St Margaret's Street, Canterbury, KENT CT1 2TU,
First Printing: 2015 First published by: Icutrain Ltd*)*

для студентів 2 курсу
спеціальність – *125 "Кібербезпека"*

Чернівці, 2021

TASK 1

CYBERSECURITY AND 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 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*[1]. You might think that to a greater or lesser extent, you have opted out of an overreliance 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 election 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. 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.*

On the contrary:

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

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.

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[2] 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 sit 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

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)[3] 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 people's 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[4]. 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[5] 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.

VOCABULARY EXERCISES

1. Fill in the tables using the dictionary. Study the words and their definitions.

Vocabulary notes

Word (combination)	*Definition*	*Ukrainian equivalent*
allegiance	loyalty or commitment to a superior or to a group or cause	
apparent	clearly visible or understood; obvious	
astounding	surprisingly impressive or notable	
barrage	an overwhelming number of questions, criticisms, complaints, etc. delivered simultaneously or in rapid succession	
boost	help or encourage (something) to increase or improve	
boundary	a line which marks the limits of an area; a dividing line	
competitor	an organization or country that is engaged in commercial or economic competition with others	
concern	a cause of anxiety or worry	
contemplate	think about	
custom made	made or done to order for a particular customer.	
cutting-edge	highly advanced; innovative or pioneering	
decision-making power	the ability of reaching decisions, especially in a large organization or in government	
defer to	submit to or acknowledge the merit of	
diminish	cause to seem less impressive	

	or valuable	
endure	suffer (something painful or difficult) patiently	
equation	a statement that the values of two mathematical expressions are equal (indicated by the sign =)	
failsafe	unlikely or unable to fail	
fuzzy area	difficult to perceive; indistinct or vague	
geek	a knowledgeable and obsessive enthusiast	
highlight	draw special attention to	
humble	having or showing a modest or low estimate of one's importance	
in-house	done or existing within an organization	
intrusive	causing disruption or annoyance through being unwelcome or uninvited	
leak	an intentional disclosure of secret information	
lure	tempt smb. to do something or to go somewhere, especially by offering some form of reward	
mess up	cause something to fail or be spoiled	
on the line	at serious risk	
ongoing	continuing; still in progress	
opt out	choose not to participate in or carry on with something	
option	a thing that is or may be chosen	
outpace	go, rise, or improve faster	

	than…	
roll out	to make a new product, service, or system available for the first time	
sensitive	kept secret or with restrictions on disclosure to avoid endangering security	
shrink wrap	a thin, transparent plastic material that tightly covers the thing that it is wrapped around, used for protecting goods when they are being transported or sold	
smug	having or showing an excessive pride in oneself or one's achievements	
sustain	strengthen or support physically or mentally	
unrest	a state of dissatisfaction, disturbance, and agitation in a group of people, typically involving public demonstrations or disorder	
uptake	the action of taking up or making use of something that is available	
weaponry	weapons regarded collectively	

CS Terms

Word (combination)	*Definition*	*Ukrainian equivalent*
breach	a break in the security system	
bypass	go past or round	
damage	harm that impairs the value, usefulness, or normal function of something	
diverse	showing a great deal of	

	variety; very different	
electromagnetic pulse	an intense pulse of electromagnetic radiation, esp. one generated by a nuclear explosion and occurring high above the earth's surface	
flexibility	the ability to be easily modified	
hack	gain unauthorized access to data in a system or computer	
host	a computer that mediates multiple access to databases mounted on it or provides other services to a computer network	
intentional	done on purpose; deliberate	
intervention	interference into action or process	
leverage	use (something) to maximum advantage	
mainstream	the ideas, attitudes, or activities that are shared by most people and regarded as normal or conventional	
malicious	characterized by malice; intending or intended to do harm	
mandate	give (someone) authority to act in a certain way	
mitigate	make (something bad) less severe, serious, or painful	
mount	establish; set up	
remediation	the action of remedying something, in particular of reversing or stopping damage	
retrieve	find or extract (information	

	stored in a computer)	
revenue	income, esp. when of a company or organization and of a substantial nature	
scope	the extent of the area or subject matter that something deals with or to which it is relevant	
system outage	a period when a power supply or other service is not available or when equipment is closed down	
threat	the possibility of trouble, danger, or ruin	
unauthorized access	viewing of any form of confidential information without permission	
update	make (something) more modern or up to date	
vulnerability	the quality or state of being exposed to the possibility of being attacked or harmed	

2. (a)Translate the italicized passages including those in the boxes into Ukrainian paying particular attention to the terminological units and CS terms usage; (b) learn the definitions of the terms.

3. The Internet Research:

Browse the Internet for some information concerning the things marked in the text with superscript numerals (1-5). Make up a short presentation using the information found.

Mind!

Split Infinitive

A split infinitive is created by placing an adverb or adverbial phrase between the '*to*' and the verb: for example, to *boldly* go, to *casually* walk, to *gently* push, to *diligently* read; to *happily* write; to *scientifically* illustrate.

Although split infinitives have been widely condemned in grade-school classrooms,

they're common in writing of all kinds.

When to avoid split infinitives. When moving the adverb to the end of a phrase doesn't cause confusion or change the sentence's meaning, it's a good idea to keep the infinitive intact. For example: *He urged me to casually walk up and say hello.*

There's no reason why this sentence couldn't be:

He urged me to walk up casually and say hello.

It's also a good idea to avoid splitting infinitives too widely:

For example: *This software allows your company to quickly, easily, and cost-effectively manage all tasks.*

One possible revision:

This software allows your company to manage all tasks quickly, easily, and cost effectively.

When to split infinitives. Infinitives should be split when the adverb either needs emphasis or wouldn't work anywhere else in the sentence. For example: *They're expected to gradually come down in price to about $50 to $75 each.*

Placing *gradually* anywhere else in this sentence (*They're gradually expected …* ; *… come down in price gradually to about …)* would create awkwardness and confusion. Another example: *Caterpillar plans to more than triple employment at its four-year-old diesel generator plant in Newberry.*

Here, the phrase *more than* would not work anywhere else in the sentence. Try it, and you'll see.

(http://grammarist.com/grammar/split-infinitives/)

4. Find in the text above the sentences with split infinitives. Write them out and analyze their usage according to the rules above.

TASK 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[1], 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***[2]*,* ***botnets***[3]*,* ***computer viruses***[4]*,* ***ransomware***[5]*,* ***scareware***[6]*,* ***spyware***[7]*,* ***trojans***[8] *and* ***worms***[9]*, 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****.*

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: (1) verify the event is real and identify the affected areas. (2) Contain the problem (usually by isolating, disabling or disconnecting the affected pieces). (3) Understand and eradicate the root cause. (4) Restore the affected components in their fixed state. (5) 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.

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[10] 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.

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.

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

VOCABULARY EXERCISES

1. Fill in the tables using the dictionary. Study the words and their definitions.

Vocabulary notes

Word (combination)	*Definition*	*Ukrainian equivalent*
span	the length of time for which something lasts	
(security) posture	a particular approach or attitude	
stacked	placed in a queue for subsequent processing	
silo	a system, process, department, etc. that operates in isolation from others. Funds, assets, or anything else kept separate from other funds or assets of a similar type	
asset	in accounting: anything of value that a person or firm buys.	
drawback	a disadvantage or problem	
impact	a marked effect or influence	
to trigger	to cause (a device) to function	
inconspicuous	not clearly visible or attracting attention	
to eradicate	to destroy completely; put an end to	
ultimately	finally; in the end	
shortcoming	a fault or failure to meet a certain standard	
ransom	a sum of money demanded or paid for the release of a captive	
extortion	the crime of obtaining something from someone,	

	especially money, by using force or threats	
objective	a thing aimed at or sought; a goal	
goal	the object of a person's ambition or effort; an aim or desired result	
expertise	expert skill or knowledge in a particular field	
offensive	an organized and forceful campaign to achieve something	
to be subject to	to be affected by or possibly affected by (something); likely to do, have, or suffer from (something)	
to be prone to	to be likely to or liable to suffer from, do, or experience something, typically something regrettable or unwelcome	
counterpart	another person or thing that has a similar function or position in a different place	
rogue	a dishonest or unprincipled man	
core	the part of something that is central to its existence or character	
to audit	to conduct a systematic review of	
complacent	showing smug or uncritical satisfaction with oneself or one's achievements	
to be deemed to	if something is deemed to have a particular quality or to do a particular thing, it is	

	considered to have that quality or do that thing	

CS Terms

Word (combination)	*Definition*	*Ukrainian equivalent*
root causes	a factor that caused a nonconformance and should be permanently eliminated through process improvement	
IT infrastructure	a set of components that are the foundation of an IT service: typically physical components but also various software and network components	
network segment	a part of the network	
identity (password) credentials	a qualification, achievement, quality, or other information about an *identity* such as a name, government *ID*, home address	
perpetrator	trespasser, disturber	
disruption	disturbance or problems which interrupt an event, activity, or process	
credibility	the quality of being trusted and believed in	
to outsource	to obtain (goods or a service) by contract from an outside supplier	
case study	a process or record of research in which detailed consideration is given to the development of a particular situation over a period of time	

2. (a)Translate the italicized passages including those in the boxes into Ukrainian paying particular attention to the terminological units and CS terms usage; (b) learn the definitions of the terms.

3. <u>The Internet Research:</u>

Browse the Internet for some information concerning the things marked in the text with superscript numerals (1-10). Make up a short presentation using the information found.

TASK 3

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. […]

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[1]. Intelligence about technology is beginning to be recorded on something called a DQ or Digital Quotient[2]. 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.*

[…] 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 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 be 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. There are six main groups of cybersecurity tasks and skills to consider, with examples of roles underneath:

Cybercecurity Functions	**Examples of roles within a function**
1. Management	Chief Cybersecurity Officer; Cyber Risk Manager; Cybersecurity Architect
2. Cyber Audit and Assessment	Audit Manager; Auditor; Assessment Specialist
3. Event Monitoring and Alerts	Security Incident and 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 and 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 (CCO) to exist on the board of any organization. Within a few years, it will be rare for any organization not to have one. The 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 CCO. 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 CCO 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 CCO role or remain separate, depending on the size of the company. A good way to think simply about a CCO 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 **risks** 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 and 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.

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 AND 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 if 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 AND 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 and 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 are 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 s*et 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 configure and maintain the digital gateways and corridors.

Intrusion Detection & Prevention Specialists 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 role advises on the security risk process design and provides consultative assistance to the business during this process.

ENVIRONMENT TESTING

This is to help sustain a secure digital landscape, there are certain additional tests carried out.

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

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 codemaker).

Cryptanalyst analyzes encrypted information to decrypt and reveal the information. *Essentially, this role is an encryption code-breaker. This can be especially useful in antimalware 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.

VOCABULARY EXERCISES

1. Fill in the tables using the dictionary. Study the words and their definitions.

to understand and keep up with the changes	
to be responsible and accountable	
an executive strategic focus	
board level responsibility	
to have the full confidence of	
a continual eye on emerging technologies	
a keen sense of risk	
external diligence checks	
the cumulative set of open risks	

to crosscheck the security and integrity of all key technologies, suppliers and processes	
tracking and reporting on the activities	
significant control gaps	
to be aligned	
attempted intrusions into the network	
to form status dashboards and automated alerts	
to help advise, augment or educate	
natural disasters and technical resilience	

2. Explain the meaning of the following CS terms in English. Use the dictionary to find the definitions if necessary. Give the Ukrainian equivalents of the terminological units below.

1) governance; 2) digital failure; 3) digital landscape; 4) policies; 5) procedure; 6) (cyber)risk; 7) security architecture; 8) denial of service; 9) distributed denial of service; 10) ethical hacker; 11) zero-day; 12) backdoor; 13) business continuity plan; 14) technical disaster recovery plan.

3. Give the full versions of the following acronyms.

CCO – _____

CISO – _____

DoS – _____

DDoS – _____

EGGE – _____

4. (a)Translate the italicized passages including those in the boxes into Ukrainian paying particular attention to the terminological units and CS terms usage; (b) learn the definitions of the terms.

The Internet Research:

Browse the Internet for some information concerning the things marked in the text with superscript numerals (1-2). Make up a short presentation using the information found.

TASK 4

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 and Consent;
- Cybersecurity Defense Points: Data, Devices, Applications, Systems and Networks;
- Cybersecurity Control Types: Physical, Procedural, Legal and Technical;
- Cybersecurity Control Modes: Preventive, Detective and 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.*

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[1], 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 won'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 physical, 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 two physically identical computers. However, if one of those computers is empty and the other contains pre-stock market announcement or 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 four 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 building 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 two 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 two 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 four 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 three 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*** – *t*o protect the device **before** any event happens.

• ***Detective controls*** – to monitor and alert me **in** the event something happens.

• ***Corrective controls*** – *t*o 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;*
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 three 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 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.

VOCABULARY EXERCISES

1. Fill in the tables using the dictionary. Study the word combinations and be able to explain their meaning in English.

low value information	
to acquire financial or political gain	
at somebody's expense	
to attack or compromise a digital device	
inherent value	
proportionate to value	
to take more precautions	
to set access restrictions	
unauthorized modification	
sensitivity to disruption or outage	
a fully redundant failsafe	
retention and notification	
the most fundamental cornerstone	
a collection of devices, wiring and applications	

to be intercepted or copied	
pre-stock market announcement	
a logical priority order	
an incentive to promote good practices	

2. Explain the meaning of the following CS terms in English. Use the dictionary to find the definitions if necessary. Give the Ukrainian equivalents of the terminological units below.

1) preventive controls; 2) corrective controls; 3) data; 4) physical security; 5) integrity; 6) devices; 7) applications; 8) detective controls; 9) confidentiality; 10) availability; 11) consent; 12) advanced persistent threats; 13) loss (in this context); 14) cyber defense points.

3. Give the full versions of the following acronyms.

CIA – _____

APTs – _____

4. (a) Translate the italicized passages including those in the boxes into Ukrainian paying particular attention to the terminological units and CS terms usage; (b) learn the definitions of the terms.

5. The Internet Research:

Browse the Internet for some information concerning the things marked in the text with superscript numerals. Make up a short presentation using the information found.

TASK 5

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, create 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. […]

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.

[…] 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 be 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 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.

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.

VOCABULARY EXERCISES

1. Fill in the tables using the dictionary. Study the word combinations and be able to explain their meaning in English.

a substantial contributor to	
unanticipated failures	
disinterested and disaffected personnel	
insider knowledge	
a single point of accountability	
onsite security audit at a supplier	
valid items	
the betterment of the staff	

good team workmanship	
to stay on top of the subject area	
to hold and maintain current certifications from a recognized authority	
to identify and report risks	
to create substantial impact into a formal framework	
to seek opportunities to take personal advantage	
the whistle blowing process	
self-assessment criteria	
to use knowledge and access for personal gain	
to try and re-use the same credentials	
a few privileged and trusted people	
to be badly burned by the failure of trust issue	
cornerstone in the area of security	

2. Explain the meaning of the following CS terms in English. Use the dictionary to find the definitions if necessary. Give the Ukrainian equivalents of the terminological units below.

1) espionage techniques; 2) body language; 3) culture (*in this context*); 4) silo thinking; 5) escalation paths; 6) rogue insiders; 7) security awareness; 8) rationale; 9) social engineering; 10) propensity; 11) pre-meditated; 12) instigate.

3. Translate the italicized sentences into Ukrainian.

4. The Internet Research:

Browse the Internet for some information concerning the things marked in the text with superscript numerals. Make up a short presentation using the information found.

TASK 6

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.

[…] 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 6 we looked at ***cyber defense points*** and identified five major categories:

1) **Data** – any information in electronic or digital format.

2) **Devices** – any hardware used to create, modify, process, store or transmit **data**. Computers, smart phones and USB drives are all examples of devices.

3) **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.

4) **Systems** – groups of applications that operate together to serve a more complex purpose.

5) **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: (1) An access route to higher security areas; (2) To subvert the lower security zone assets for ***denial of service*** attacks; (3) 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.

Infection.

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 *– seeking 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) removing 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. […] *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 and 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 antimalware 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.*

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 use 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.

VOCABULARY EXERCISES

1. Fill in the tables using the dictionary. Study the word combinations and be able to explain their meaning in English.

be completely circumvented	
to sub-divide the attack surface	
discrete management of each section	
to subvert the lower security zone assets	
to allow the malware to re-install itself	
to disable or bypass other security measures	
to be commenced	
to temporarily store data	
to perform executive control over an electronic device	
to exfiltrate stolen information	
to perform fast, repetitive tasks	

to coordinate, update and direct what the malware does	
to protect, serve or subvert the community of devices	
an adequate and appropriate spread of security defenses	
to isolate the attack (quarantine the malware)	
to identify and manage rogue software	
to scan any uploaded files for threats	
to bypass other security defenses, masquerading as application data	
to act as gatekeepers at the borders of each network	
to indicate the destination, source and type of payload	
to block and log (record) any malicious or otherwise unwanted streams of information	
inadvertent operational disruption	

2. Explain the meaning of the following CS terms in English. Use the dictionary to find the definitions (in the context of cybersecurity) if necessary.

1) Infection; 2) persistence; 3) boot; 4) exploitation; 5) inbound and outbound communication; 6) bot; 7) updates; 8) infiltration point; 9) decapitation; 10) signature; 11) packet; 12) protocol.

3. Translate the underlined sentences into Ukrainian.

4. Translate the following word-combinations. Mind the use of nouns in the attributive function.
1) attack surface; 2) information security professional; 3) target area; 4) network segmentation; 5) security zone; 6) attack exploit; 7) security area; 8) attack process; 9) definitions section; 10) security measure; 11) command level access; 12) communication option; 13) intrusion detection and prevention systems; 14) protocol format; 15) data loss prevention; 16) vulnerability assessment; 17) attack communication; 18) business rules; 19) information classification; 20) privacy regulations.

5. (a)Translate the italicized passages including those in the boxes into Ukrainian paying particular attention to the terminological units and CS terms usage; (b) learn the definitions of the terms.

TASK 7

EVOLVING ATTACK AND DEFENSE METHODS

(based on Chapter 9)

[…] 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[1], 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 – the full range of policies, procedures and specific controls that the executives 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 – the results from processes used to verify that ***governance*** items are being followed and to identify any gaps.

• ***Risk*** information – 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 antimalware 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***[2] 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.

• 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.

VOCABULARY EXERCISES

1. Fill in the tables using the dictionary. Study the word combinations and be able to explain their meaning in English.

generic user and password permissions	
to deploy critical, interim updates to software on digital devices	
zooming in and out on a map	
system is designed to pull together	
to keep their organization working within acceptable boundaries	
to substantially and materially impact the organization	
collecting and synchronizing this highest level information	
creating an informed view of the overall security position	

to pull information from more granular sources of security coordination software	
pull together information about information traffic and attempts at intrusion	
to measure, manage and monitor identified problems through to closure	
make up the majority of paths to infection	
to more effectively evade anti-malware	
unintentional use by gifting infected devices to targeted employees or suppliers	
growth of mobile computing	
intrusion detection and prevention software	
to help capture, trace and prosecute attackers	
to lure, identify and trace would-be attackers and their malware	
to be fully decrypted and inspected	
a holistic view of security	

2. Explain the meaning of the following CS terms in English. Use the dictionary to find the definitions (in the context of cybersecurity) if necessary.

1) physical tokens; 2) a software ‘patch’; 3) security coordination software; 4) information traffic; 5) legitimate source; 6) secure, encrypted protocols; 7) web server; 8) web browser; 9) USB connection ports; 10) hidden server; 11) data retention; 12) to patch.

3. (a)Translate the italicized passages including those in the boxes into Ukrainian paying particular attention to the terminological units and CS terms usage; (b) learn the definitions of the terms.

4. The Internet Research:

Browse the Internet for some information concerning the things marked in the text with superscript numerals. Make up a short presentation using the information found.

Appendix

Case Study Examples

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***[1] thumb drives. These were able to be physically taken in and out of the facility.

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 prescreening 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.

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[2] layer.

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.

*[1]**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.*

*[2]**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.*

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's Apstls' 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**[3].

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 nonsensitive 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[4].

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.

[3]***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.*

[4]***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.*

[5]***doxxing*** *(also* ***doxing****) – publicly exposing personal information on to the Internet. Thought to be based on an abbreviation of the word 'documenting'.*