Cyber Security Primer.

What is Cyber Security?

To answer this question, we need to first understand what is Cyber? Put simply, this is the new modern word for a world in which information is stored, processed, and accessed, specifically, in this constantly ever on and connected age, within the electronic environment. Before it was known as Cyber Security, we used to call the discipline Information Security. The two terms are today interchangeable but was changed specifically to encompass the wider scope of the people, processes, environments, and technology that interact with this information.

So, what about the security part? Well, you have heard of the saying that knowledge is power. That being the case, then information is an attractive commodity that other people want to possess and that, therefore, needs to be protected. That protection provides a sense of security when dealing with this knowledge commodity, but needs to be constantly monitored, updated, managed, and controlled. An attacker only needs to get it right once, a defender needs to protect against all forms of attack and to get it right 100% of the time. The truth here is that if you can build it electronically, you can break it electronically (eventually). Cyber security is therefore all about assessing the risk that such an attack or simple mistake might occur and lead to a successful loss of information, what the impact of that loss might be, and to put into place measures (security) that might reduce that risk to a manageable level. It is also about how that risk, once reduced is managed going forward such that a mistake/attack can be detected and responded to thus reducing the impact of loss.

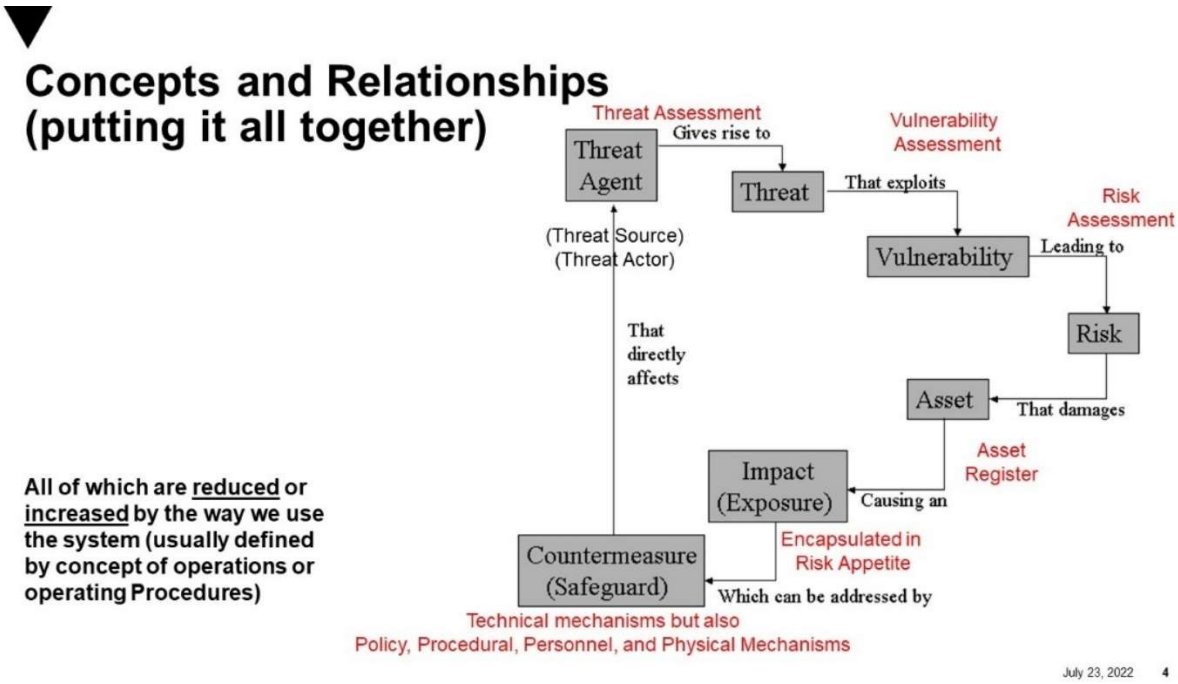
Risk Assessment

As we have already discussed if we have anything of value there is always the potential for others to want to possess that valued item (we call these ***Assets*** and it not only includes the information but key personnel, the equipment on which it is stored, key sites and so on). So, the first stage of any risk assessment is to produce a list (catalogue) of assets that we value. Alongside that, we also need to determine a measure of what that value is (these measures can be as simple as high, medium, low) and what the impact of their loss is (from “critical, my world will end,” to “I don’t care”).

Having determined “what have I got” and “how valuable is it” we now need to understand who might be interested in possessing that information and how skilful they might be at accessing it (a ***Threat***). How skilful depends on how well motivated the attacker is, what resources they have, what opportunity there is for them to conduct the attack and so on. These considerations (we call that a ***Threat Assessment***), and those of trying not to get caught, may drive an attacker to use somebody else (willingly, or unknowingly) to perform the actual attack on their behalf. In technical terms we might therefore discuss a ***Threat Source*** (Uncle Bill) and a ***Threat Actor*** (Cousin Maude). Of course, if clever enough, Uncle Bill could be both the Source and the Actor!

Now if the information is written on a piece of paper sat in unobstructed view on a desk, it is obviously more vulnerable than if it were locked in a vault within Fort Knox. So having catalogued the Threat and its viability (likeliness to succeed) to then need to catalogue the ***Vulnerability*** (this is where software updates come in for example – a vulnerability is identified and corrected) and to determine the level of ***Risk*** to our Assets. Vulnerability can be described as a weakness in a mechanism that threatens the **Confidentiality**, **Integrity**, or **Availability** (the **CIA Triad**) of an Asset. In quite simple mathematic terms ***Risk = Threat x Vulnerability x Asset Value.***

Having calculated all of this (we call it a **Risk Assessment**) we can now look at what we can do about this. We can simply put something in place (**Countermeasures**) to reduce the risk to a manageable level (to make it difficult enough for an attacker, or to make the risk of capture/exposure so high that they go away and seek a less risky target). We call these measures to reduce the risk, ***Risk Treatment***, and the process for managing any risk that remains (***Residual Risk***) is called ***Risk Management***



Risk Treatment and Risk Treatment Plan

As identified above, the consideration of safeguards or countermeasures we can put into place is developed and implemented through what we call a ***Risk Treatment Plan.***

As with all things in life there are layers in which we can apply these safeguards. We can look at the Physical Environment in which the information is accessed, stored, and processed (***Physical Measures***). This is where locks on doors, passes, security guards, environment controls and the like are considered and implemented.

Alongside that we need to look at who might legitimately be accessing our Assets (***Personnel Measures***): how we select these people and validate their loyalty, motivation, and integrity; how we train and develop them; what level of access they require; and what level of personnel management is required.

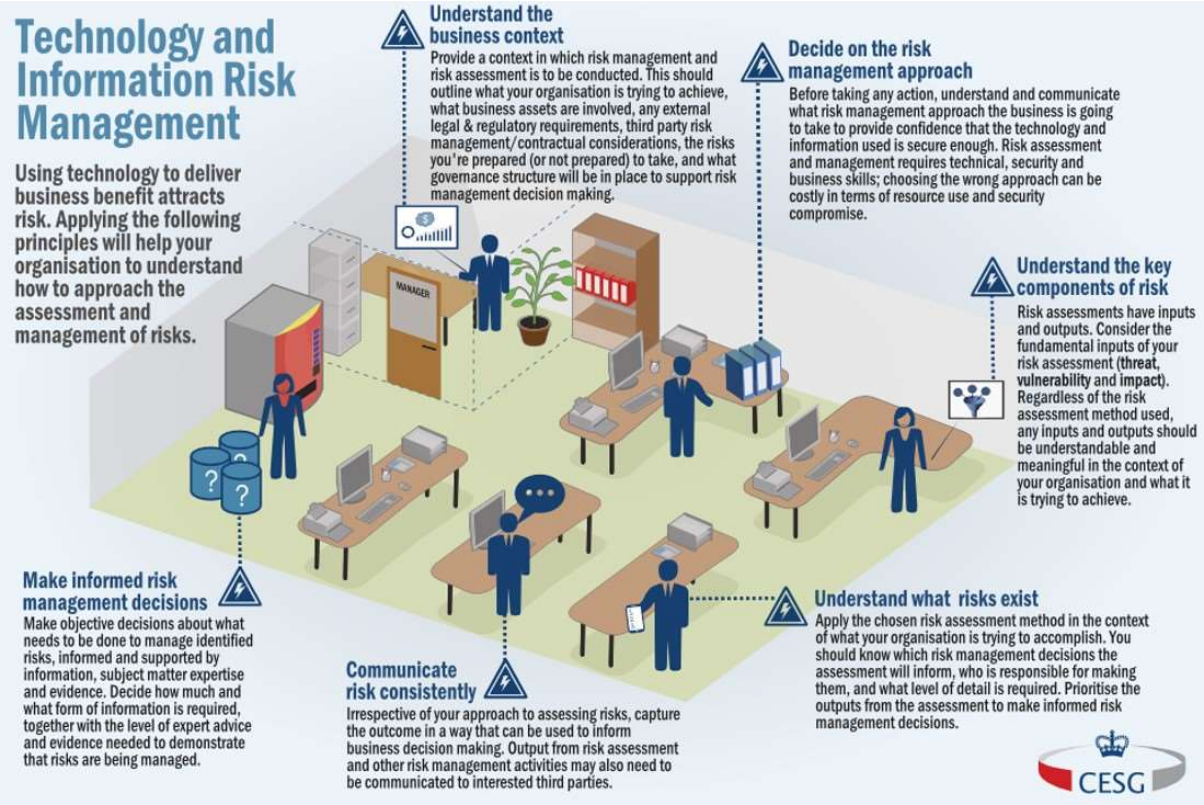
To help us identify, implement, and manage these two sets of measures two key areas considered by businesses are Policy (what is the security strategy for defending our assets), and procedure (how do people access our assets within that physical environment in line with that policy). We call these ***Policy Measures*** and ***Procedural Measures*** (see reference to concept of operations and operating procedures in above diagram) which can again be implemented at various levels – what do we do at National level, in this school/business/government department or what do we do locally, in the

library/cybercafé, at home, in the Office, in a public space (airport lounge/train station/favourite green space), or IT classroom. These have in the past been referred to as the Global and the Local security environments – terms no longer used but useful here to illustrate the point.

Only then do we consider how we can use technology to support these other measures and to complete the picture. (***Technology Measures***). By getting the policy, procedural, personnel, and physical measures in place first, we can reduce the burden on the technology measures required. For example, if I only use information on paper in a locked cupboard in my bedroom, do not let anyone in my room, and my day enforces that, then it is far less risk than if I publish it on Facebook and allow anyone to access it.

Sometime the technology does come first, however. Consider, if my dad just bought me a new iPad, so of course, all the above has a starting point of "How do I do this on an iPad." A company/school that only uses Apple Mac technology or the Linux/Microsoft Operating System where the starting point is again how do I do this on this environment (particularly if legacy (old/superseded) equipment). Finally, a laptop in a highly classified Defence/government environment, a design laptop in industry, or a shared desktop in a cyber café or a local library where some/none of the above are already implemented and requires review and update as opposed from starting from nothing. Where the technology does come first, reviewing/implementing the above measures may help to reduce the management overhead and costs of protecting that asset in that technical environment.

Risk Management



At the end of Risk assessment and risk treatment there is always a measure of residual risk – remember we do not attempt to remove all risk – an impossible task – but only to reduce risk to a

manageable level – that means there is still risk that needs to be managed. Above is a government slide that covers this aspect.

Risk management is the discipline that says what do we do to manage that residual risk. Here we can take several positions: we could simply ignore it and hope it will go away, accept it as manageable (and here we have options as to how we manage the risk), or reject it. If we reject the idea that the risk can be managed, we again have several options, we can go through the cycle again tightening up on the risk treatment, we can take out insurance against the loss, and so on. Here you will hear term such as **Risk Avoidance**, **Transfer of Risk**, and **Risk Management**

Once we have implemented our Risk Treatment Plan (safeguards/countermeasures) we need to regularly (at least annually) review our risk assessment as part of that risk management for continued relevance and against current changes to the various environments.

Risk management strategies include:

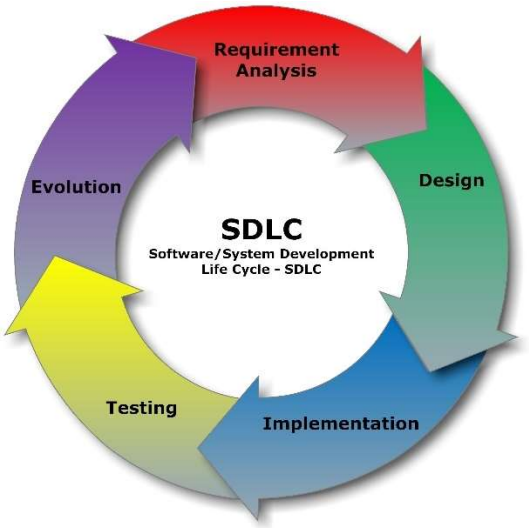
- **Remediation:** Implementing a control that fully (or nearly) fixes the underlying risk (Example: Apply a patch for an identified IT item where critical assets are stored). This does not mean we do not need to revisit those solutions and to change (increase/reduce/replace) them
- **Mitigation**: Reduce the likelihood/impact of the risk, but not fixing it entirely. IT Item (Example instead of patching the vulnerability, implement a firewall rule that only allows specific systems to communicate with the vulnerable service).
- **Transference**: Transferring the risk to another entity so your organization can recover from incurred costs of the risk being realized. (Example: purchase insurance that will cover any losses that would be incurred if vulnerable systems are exploited. Note that this should be used to supplement risk remediation and mitigation but not replace them altogether).
- ***Risk acceptance***: Not fixing the risk. This is appropriate in cases where the risk is clearly low and the time and effort it takes to fix the risk costs more than the costs that would be incurred if the risk were to be realized. This does not mean that you do not track attempts to exploit such a risk and take appropriate incident management activity – covered later. (Example: identified vulnerability on a server but there is nothing sensitive on that server; it cannot be used as an entry point to access other critical assets, and a successful exploit of the vulnerability is overly complex).
- **Risk avoidance**: Removing all exposure to an identified risk (Example: equipment with operating systems (OS) that are about to reach end-of-life and will no longer receive security patches from the OS creator. Where this equipment processes and store both sensitive and non-sensitive data it could be migrated to newer, patchable equipment to avoid exposure whist continuing to run and process non-sensitive data on the old equipment while a plan is developed to decommission them and migrate the non-sensitive data to other equipment).

The role of Cyber Security in the Product/System lifecycle

The system-development life cycle (SDLC) enables engineers to transform a newly developed project into an operational one. SDLC is a multistep, iterative process, structured in a methodical way (there are similar diagrammatic representations and acronyms). This process is used to model or provide a

framework for technical and non-technical activities to deliver a quality system which meets or exceeds business expectations or to manage decision-making progression.

Traditionally, the systems-development life cycle consisted of five stages. That has now increased to seven phases. Increasing the number of steps helped systems analysts to define clearer actions to achieve specific goals. Like a project life cycle (PLC), the SDLC uses a systems approach to describe a process. It is often used and followed when there is an Information Technology (IT)or Information (cyber) Security (IS) project under development. The life cycle approach is used so to support understanding of the activities involved within a given step and indicate that at any time, steps can be repeated, or a previous step can be reworked when needing to modify or improve the system.



1. **Planning**: To determine the scope of the problem to be addressed and solution spaces to address those problems. This stage also helps to assess and articulate the solution spaces identified and their associated resources, costs, time, benefits to determine the best course of action to address the problem identified.

2. **Systems Analysis & Requirements Capture**: To identify and consider the requirements (functional and non- functional) of the project or solution. It is also where systems analysis takes place covering analysis of business, technology, and user needs leading to development of a solution that meets expectations in these areas. The outcome is recommended solution and assessment of how well requirements are met, and any areas where some compromise in those requirements is required, why, the impact, and alternatives if necessary. This will produce an initial high-level design as one of the main outputs.

3. **Systems Design**: To describe in detail the necessary specifications, features, and operations that will satisfy the requirements of the proposed system solution. This will refine the High-level design and develop a detailed (low-level) design of the chosen solution space.

4. **Development**: This marks the end of the concept and design stages and the start of production including installation and change. At this point the detailed design is implemented, refined, and updated in a development environment. All supporting information how requirements are met, issues/weaknesses within the solution space, and so on are also identified and communicated.

5. **Integration and Testing**: Systems integration and system testing (in the test environment which simulates as near as possible the operational environment) of programs and procedures determines if the proposed design "does what it says on the tin" (meets the initial set of business goals and design requirements).

6. **Implementation**: This is the stage where the operational code and equipment is built and configured in the operational ("Live") environment. Here the project is effectively put into production as data and components are migrated into the environment in which they are to operate.

7. **Operation and Maintenance**: Here is the stage at which the users and administrators are provided access to the system and begin to fine tune the system to meet administration and use requirements boosting performance, adding new capabilities, or meeting additional system requirements. This stage continues right up to and including decommissioning of a system when it is no longer of use.

As can be seen from the above there are many disciplines at plan in each of these stages this is also true of the Cyber–Security Lifecycle which follows a similar lifecycle (security built-in), and mimics many of those disciplines but with specific Information (cyber) security Knowledge.

Cyber Security roles

These roles include:

- **Cyber Security Analyst**: Plan, analyse and execute cyber security strategies and plans. Synonymous with Enterprise Security Architect.
- **Vulnerability Assessor**: Spot vulnerabilities and solve them. Sometimes referred to a General (security) Risk Management consultant (GRMC).
- **Cyber Security Auditor**: Find weak spots in the security profile of the system before an attacker can find and exploit them. This may be performed under the management of a Security Controller or the ITSHC/Pentest manager
- **Cyber Security Architect:** As with normal systems disciplines this role is conducted at various levels.
    - At the top is the **Enterprise Security Architect,** whose role is to ensure that the security architectural design meets the business need of the enterprise.
    - Next is the **Systems Security Architect,** whose role is to ensure that the security solution can be integrated with the existing systems.
    - Below this is the **Security Solution Architect**, whose job is to ensure that the security requirements are met by the proposed solution having identified and included the appropriate countermeasures.
    - Finally, there is a **Technical Solution Architect**, whose job is to assist the implementation team in the build and configuration of proposed solution.
- **Cyber Security Administrator:** keep security systems running smoothly. This function is usually fulfilled by the Cyber Security Team, or SOC, Manager.
- **Source Code Editor:** Ensure code accuracy and (security) safety prior to release (see threat hunter within the SOC Team)

- **Cyber Security Consultant:** provides advice and implementation of security solutions. Synonymous with Security Solution Architect.
- **Cyber Security Engineer:** Assist in the building and implementation of the security elements of IT systems design. Synonymous with Enterprise Security Architect. Synonymous with Technical Solution Architect.
- **Cyber Security Incident Responder:** Monitor security threats and actively respond to them
- **Forensic Expert:** Protect and assist in law enforcement through a scientific study of security.
- **Penetration Tester:** Attempt to penetrate the computer and network systems to pre-emptively discover operating system and firmware vulnerabilities, service and application problems, improper configurations and so on. You may see the term Information Technology Security Health Check (ITSHC) and Penetration Test use interchanged. The basic difference is that an ITSHC tests to see if a system behaves as it should and if weaknesses are exploitable. This is described as non-destructive (positive – does it work) testing, whereas Penetration testing goes that step further to see if discovered vulnerabilities can be exploited and what damage this can cause and is therefore considered destructive (negative – can I break it) testing.
- **IT Cyber Security consultant**: Meets with clients providing advice on how best to protect an organisation's cyber security objectives efficiently and cost effectively.
- **Chief Information Security Officer (CISO):** This is typically a mid-executive level role responsible for overseeing the general operation of security. The CISO is personally responsible for planning, co-ordinating, and directing all IT, network, and data security needs of the business and the employers.
- **Security Controller (SC)**: This role is responsible for the day-to-day management and administration of the corporate security needs. This role has primary concern for the physical, personnel, and procedural security mechanisms including control of secure documentation/information. In larger organisations, a **Site Security Controllers (SSC)**, and a small admin team may supplement this role.
- **Security Awareness Trainer**. In larger organisations, a team member may assist the CISO and SC where regular and multiple awareness training activities are needed, and security training records need keeping. The role may also contribute to incident management.
- **Security Standards Manager/Compliance Officer**. Again, in larger organisations the need to keep track of national and international standards, to implement change, and track compliance may be supported by a member of the security team employed to ensure regular monitoring and to ensure legal compliances are met. The role may also contribute to incident management.
- **ITSHC/Pentest Manager**. In larger development organisations where there is a large amount of sub-contracted (independent and verified) ITSC/Pentest activity, it is useful to have a local resource to assist in the administration of on-site testing, management of reports, and development of a remediation plan.

More recently, particularly with the rise of development, Security, and Operational (DevSecOPs) teams, a Security Operations Centre (SOC) may regularly be provided in support of operational security thus providing the following roles and functions: L1 Monitoring team. L2/L3 SOC analysts, incident responders, cyber service desk, forensics, Security Information and Event Management (SIEM) administration, threat intelligence, threat hunter, and SOC Manager.

As can be seen, from the above

Security Processes within SDLC

Start-up Process

During the Systems Analysis and Requirements Capture phase, the Initial Technical Risk Assessment snapshot, developed as part of the planning phase is used to prioritise security risk and to logically group those risks. These are used in conjunction with Business Impact levels to produce an impact assessment (including a Privacy impact Assessment) and a model/diagram of the security solution space(s). A threat assessment is then conducted considering the maximum threat analysis and the maximum level of risk and is the used to drive an assessment of compromise methods and analysis of vulnerabilities in the proposed solution space(s).

During the design phase, the initial and developed Technical Risk assessment and the Risk Treatment processes are conducted.

Technical Risk Assessment Process

This is a 6-step process for the proposed design covering impact assessment, threat assessment, grouping any focus of interest, assessing threat levels, and vulnerability analysis resulting in a prioritised list of risks. This results in update of the initial outputs (impact assessment, risk register, and model/diagram), the threat, vulnerability, and countermeasures database content, and a risk register with various formal review points

Risk Treatment Process

Within the Risk treatment plan that follows, there are four key phases dealing with developing the risk treatment plan, Implementing the approach and development plan, conducting a residual risk analysis and gap analysis (based on the requirements and risk assessment), and producing the security case for the proposed solution.

Following on from this during Development, Integration, Testing, Implementation, and the Operation and Maintenance through to destruction, various additional cyber security resources identified above come into play.

Conclusion

Security specialists implement cybersecurity measures that protect an organization's computer networks and systems. Security specialists also secure data networks, intercept security breaches, and adjust those measures to improve security.

Whether you are searching for new or additional opportunities, information security can be vast and overwhelming. Whilst technical skills are useful, if not important, until you get hired up the ladder into senior-level jobs like chief information security officer. However, even at the entry and middle levels, a few soft skills are necessary (so do not think you will be working somewhere quietly in a corner without interacting with anyone all day).

Hard skills that are in Demand

- **Security analysis** - This role covers a broad array of skills including an understanding of both security and the specific business with its unique problems. As part of this skill set, you will need to know how to use security tools strategically to monitor various systems and

conditions, identify gaps and recommend ways to minimize the attack surfaces. According to the (ISC)2 research on hiring and retaining security talent, security analysis is by far the skill industry professionals use the most: 62 percent said it was their most commonly used skill.

- **Penetration testing** - As hackers exploit vulnerabilities to infiltrate networks and systems and data breaches continue to break records, intrusion detection has become one of the key areas of focus for organizations. Increasingly organizations hire penetration testers, or ethical hackers, to identify those vulnerabilities and to probe their information systems for the exploits attackers may find. While penetration testing is its own specialty, many other jobs (such as security analyst and information security engineer) will also often require intrusion detection and penetration testing skills.
- **Secure application development, or DevSecOps -** There is a growing trend to incorporate security into DevOps. DevOps are cross-department teams that are coming out of their silos to integrate software development and software operations. As the next step from there, DevSecOps is an emerging industry trend, particularly among large enterprises that need agile and rapid deployment for the applications they are building. Gartner forecasted that DevSecOps practices will be embedded into 80 percent of rapid-deployment teams by 2021. By comparison, only 15 percent were using DecSecOps in 2017.
- **Incident response** - Once a security incident is identified, it may take a team of different infosec practitioners and other departments to mitigate it. Many companies have an incident response plan that outlines the steps, and the security team contributes to both creating that plan and executing it when the time comes. Incident response is a multifaceted skill that draws knowledge from different areas of information security and requires a solid understanding of not only the IT ecosystem but also the specific business and its sector.
- **Cloud security -** Research by The Enterprise Strategy Group and the Information Systems Security Association found cloud skills in the top three skill areas where organizations saw a shortage. While cloud computing has matured significantly in the past few years, security remains a challenge, especially as workloads continue to be moved to the cloud.
- **Data science and analytics** - Many cybersecurity vendors are adding behaviour-based analytics, machine learning and other big-data tools into their products, from firewalls to antivirus programs. They need data scientists who can create new algorithms and models. Information security professionals who have backgrounds in data science and analytics are going to see a growing demand for their skills.
- Important **soft skills** include
    - Customer service - Information security professionals are analytical people, so they should expect to be communicating with the people whose problems they are trying to solve. Customers may be either internal, such as heads of other departments, or external, such as clients the company serves as a vendor. In a high-stakes situation, like a security incident, diffusing tension among stakeholders and working under high pressure will be part of the job. It helps to put yourself in your customer's shoes and understand their pain points.
    - Communication - Going hand-in-hand with customer service, communication is a universal skill that just about any profession requires. For a security professional, top communication skills are necessary for a variety of scenarios, whether you are deploying a new security product, troubleshooting issues, or trying to educate other employees about good cyber-hygiene.

- Collaboration - In an organization that values a security-focused culture, the IT team does not work in a silo. You may need to partner up with either your IT peers or co-workers from other departments to solve security problems. In a CompUSA survey, half of the business and IT executives interviewed noted teamwork as a top skill.
- Curiosity and passion for learning – There is never a dull moment for the information security team, and things are constantly evolving, from threats and vulnerabilities to the adversary's tactics. It helps to be naturally curious and question how and why things work, and a passion for learning will both satisfy that curiosity and help you stay ahead of threats.

Information security is a "cat-and-mouse game"— if you want to be in the lead, you will have to keep learning. There are plenty of resources that make learning easy, from online courses and certifications to industry organizations and conferences

Pros and Cons of Cyber Security Roles

- Pros
  - **Excellent salaries** for those qualified and delivering at higher levels although you may have to change employers to achieve above inflation increases.
  - **Job opportunities** are plentiful, varied, and available with a wide variety of employers See repetition below).
  - **demand** - Cyber Security Professionals are in demand
  - **Career Advancement** There are often opportunities for Career Advancement including job enrichment/job enlargement although you may have to change employers to achieve this
- Cons
  - **Demanding hours -** roles require on call or demanding hours. Cyber security professions tend to work long hours including nights and weekends spent keeping informed and up to date.
  - **Constant Learning** – to stay up to date and maintain skills and qualifications
  - **Repetition** –cyber security tasks can be repetitive and boring
  - **Lack of resources** or upper management support is a constant battle