HyperionDev

Governance, Compliance, and Roles

Task

Visit our website

Introduction

Cyber security professionals shoulder a lot of responsibility. Their security measures and skills ensure the safety of a business's enterprise and employees' personal data.

In this task, we'll look at some high-level rules governing cyber security professionals, introduce compliance frameworks, and unpack the primary roles within a cyber security team. We'll also touch on some of the basic tools used to battle cyber security threats and dig into what recruiters are looking for in entry-level cyber security professionals.

Governance at a high level

Cyber security governance aims to provide a framework that strategically outlines how an organisation enforces its security measures, calculates its operational areas of risk, and determines responsible stakeholders. Ultimately, these governing regulations exist to guide a business's overall strategic objectives, and promote an awareness of risk and a sound, effective approach to dealing with security risks. Governance also ensures clear accountability, clarifying that those accountable have appropriate steps in place to deal with risk effectively.

Many companies are adopting **principles-based governance** strategies that reduce the firm dependence on cyber security standards by organisations like the ISO (International Organization for Standardization). Principle-based governance enables organisations to adapt these cyber security standards to their business's unique needs.

Here are some of the benefits of adopting a principles-based approach to governance:

- Efficient incident response to cyber security issues.
- Rapid identification of new risks.
- A collection of high-quality test data for future security refinements.
- Fostering a company-wide awareness of cyber security threats.

Governance checklist

Here are six important steps that organisations can use to develop and enhance their cyber security governance efforts (Nigro, 2024):

1. **Establish the current state**
    - Carry out a cyber-risk assessment and a maturity assessment to get a complete overview.
    - Identify weaknesses, assess current security measures, and determine areas that need improvement.

2. **Create, review, and update cyber security standards, policies, and processes**
    - Developing cyber security governance can be straightforward, but requires effort. Take the necessary time to build a solid framework.
    - Set up clear cyber security policies, standards, and procedures to create a structure for risk management, defining roles, responsibilities, and best practices.

3. **Approach cyber security from an enterprise-wide perspective**
    - Identify and prioritise key data that needs the most protection, keeping in line with your business objectives.
    - Consider cyber security as a critical part of overall risk management, not just a technical issue.
    - Plan cyber security investments wisely, allocating resources based on risk assessment and potential impacts.

4. **Increase cyber security awareness and training**
    - With the increase in remote and hybrid work, it's essential to expand training to include not just in-house employees but also remote workers and their families.
    - It's crucial for everyone involved to understand the importance of maintaining good cyber hygiene.

5. **Assess cyber-risk analytics**
    - Develop a risk model that considers all potential threats – external, internal, and third party.
    - Contextualise and assess these risks thoroughly to understand their impact better.

6. **Monitor, measure, analyse, report, and improve**
    - Cyber security is an ongoing process. Set regular check-ins, measure important metrics, analyse data, and plan for improvements.
    - Keep the board informed about the organisation’s cyber maturity and overall cyber-risk stance.

Compliance frameworks at a high level

Compliance has become an essential pillar in modern cyber security operations. Setting a high bar for professional safety, compliance lessens the damage (both financial and reputational) **inflicted by cyber attacks**, which are becoming worryingly frequent in today's digital world.

Cyber security compliance is a set of standards and regulations issued by an agency in a supervisory role or by some other legally backed authority. These standards must be fulfilled in order to obtain full compliance. They aim to safeguard a company's **c**onfidentiality, **i**ntegrity, and **a**vailability of information (CIA, which you may remember from the previous task). Any information that has been stored, processed, or distributed must adhere carefully to the specified compliance framework.

Commonly used compliance frameworks

NIST Cybersecurity Framework: Enlists greater voluntary collaboration between the public and private sector to identify and manage cyber security threats. NIST is a highly reputable framework, and one of the most renowned for fulfilling cyber regulations.

General Data Protection Regulation (GDPR): Was brought into effect in 2016 to augment data protection for European Union citizens. This framework influences all organisations or businesses within the EU that collect personal data from EU citizens (this regulation also impacts US businesses). The framework stipulates compliance specifications on consumer data rights, data protection, and violation notification protocols.

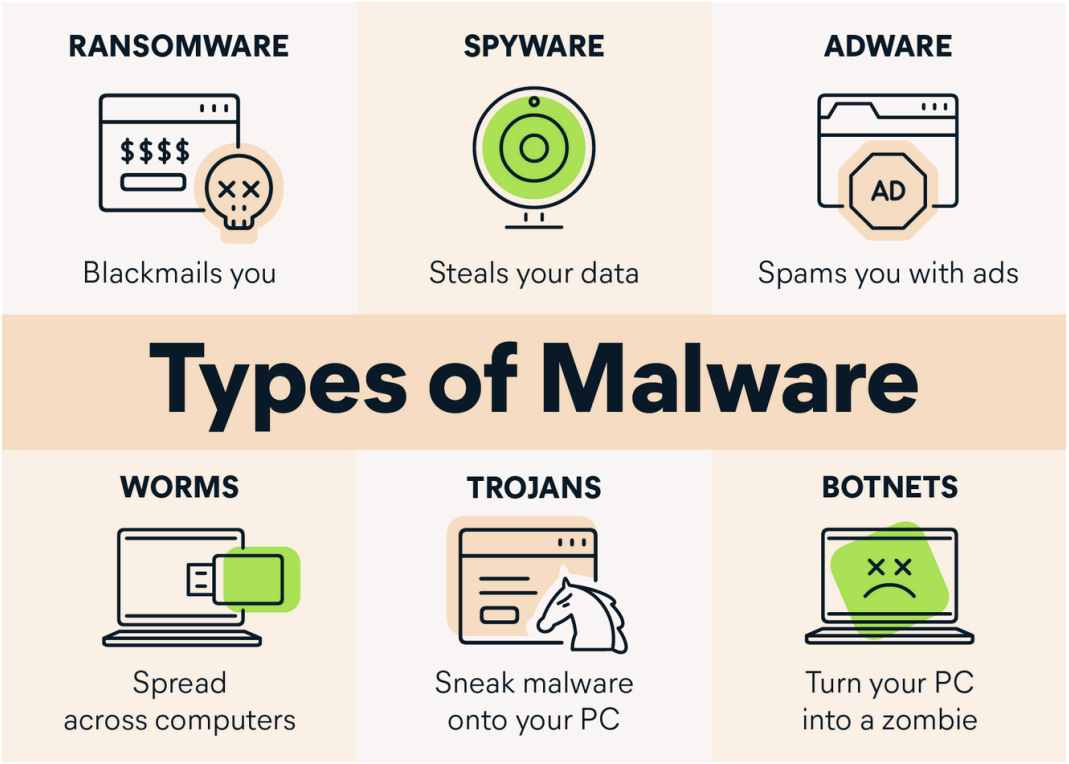
The Internet of Things Security Foundation (IoTSF) Security Compliance Framework: is an international, non-profit organisation that unites IoT security experts, network providers, product vendors, distributors and retailers, insurance providers, as well as local and other government authorities. The framework also dictates security requirements for business security, mobile applications, and cloud services.

There are many more compliance frameworks, all intended to regulate unethical conduct online. As you mature as an aspiring cyber security professional, your actions should always be informed by existing or evolving compliance frameworks, given that infringements of your company's framework could result in serious legal or financial consequences for your organisation.

Combating cyber attacks

There are a wide variety of software tools, behaviours, and processes that companies adopt to reinforce their cyber security integrity. Here are just a few:

Antivirus software: These assess a computer, IT system, or larger network for a range of threats and viruses such as worms, fileless malware, Trojan horses, rootkits, spyware, bots, and/or ransomware. Antivirus software typically runs according to frequent updates that vet the system for new threats. McAfee and Norton are just two out of many popular antivirus software brands.



Types of malware (Ivan Belcic, 2023)

Firewall: Prohibits unauthorised access to a private network. The firewall inspects all messages from an insecure connection to the user's personal or business network. It then decides if the internet traffic should be allowed or denied entry into the local network, blocking it if it does not meet a specific criteria. A firewall can be installed as **hardware or software**, although some security experts recommend a combination of both types of firewall. Talented hackers understand how to create malicious programs that circumvent the protocols asserted by a firewall.

Public key infrastructure (PKI) services: A tool that governs the identification of public encryption keys. PKI enables users and computer systems to share data safely over the internet by verifying/authenticating the recipient's identity during the exchange. SSL/TLS (secure sockets layer and transport layer security) are a version of PKI, and they are communication protocols that encrypt and secure connections between users.

Company-wide awareness: While not literally a tool, an informed and vigilant group of employees can thwart an array of sophisticated security threats. There are a number of helpful employee **security training programmes** that can be used to ensure employees are keeping current with the latest in sophisticated security breaches.

Cyber security roles

As cyber security is becoming an increasingly important function within many businesses, here are some of the most critical roles required in any effective cyber security team or organisation:

- **Security administrator:** Essential because their role spans multiple important functions. For example, it is their responsibility to establish security guidelines, and set up firewalls and malware protection software.
- **Security specialist:** Oversees the company's system security and vets its vulnerabilities.
- **Incident responder:** Detects and responds to threats. When there is a security breach, an incident responder flags the problem and employs tactics to defend against the attack.
- **Vulnerability assessor:** Similar to an incident responder, these analysts run tests on the security system to find overlooked vulnerabilities in the system.
- **Security manager:** Supervises the rest of the team. They take important decisions and oversee the whole team's work. They also design the security structure, test out the security, and respond to threats.
- **Penetration tester:** Authorised to hack a system to identify security vulnerabilities. In essence, they simulate the role of a malicious hacker. Their findings are then relayed to their manager. This is a variant of **white hat** hacking.
- **Help desk:** An entry-level role that requires knowledge of ticketing systems, requires an understanding of security precautions to protect client data, attending to various technical hardware and software issues, and a familiarity with IT diagnostics to pinpoint appropriate solutions.
- **Security consultant:** In a freelance capacity, these consultants assess a company's system(s) and propose improvements.

System administration

A system administrator or “sys admin”/“sysadmin” is responsible for managing, licensing, and maintaining or updating hardware and software within an organisation. The sys admin is responsible for employing strategies to address and resolve issues like server “downtime” and **zero-day attacks**. The sys admin may also be required to oversee the integrity of the database, and is sometimes called a “database administrator”, but their role is generally much broader than just administrating databases.

Cloud computing administration is also becoming a highly sought-after skill. The sys admin's tasks generally include provisioning, scripting, programming, security automation, and configuring and maintaining system performance, including the software running on the web servers and computer hardware. A sys admin must also be familiar with troubleshooting, establishing and managing user accounts, upgrading and patching software, and performing backup and recovery tasks.

The sys admin must command a wide range of skills, and, therefore, depending on the expectations for the role, sys admin salaries can vary from company to company. A competent sys admin should be able to solve problems in differing operating systems like Linux and Microsoft.

Extra resource

If you'd like to learn more about the system administrator role, watch this **brief overview**.

You can also inspect the job specification for an IT system administrator provided below. It is an advanced role, but by the end of this bootcamp, you may wish to pursue this as an eventual career path.

IT system administrator:

- Expand services by enhancing how tools and systems work together.
- Harden infrastructure by boosting redundancy and monitoring services.
- Apply security updates and patches to systems.
- Identify areas for improvement and weaknesses.
- Offer support to staff in your areas of expertise.

Cyber security job specifications

The salaries of cyber security professionals differ depending on the complexity of the role. Naturally, a security manager and architect would likely earn substantially more than an entry-level help desk role.

This bootcamp aims to upskill you in a variety of IT-related, programming, and architectural areas. Below, you will find two different job specifications for entry-level cyber security postings.

Cyber security incident responder:

- Handle security incidents, investigations, and forensic tasks efficiently.
- Guide and inspire a small team that responds to security incidents.
- Keep updating and enhancing our procedures and guides for responding to incidents.
- Create and maintain relationships with key people both inside our organisation and with external partners and agencies.
- Plan and oversee regular training sessions and drills on cyber security incidents.
- Serve as a coach to less experienced members of the security response team.

Penetration tester:

- Use your skills in penetration testing, preferably with some experience in incident response.
- Work with clients on various projects, such as big and small web application and infrastructure penetration tests, vulnerability assessments, and special research tasks.
- Perform tests and assessments on applications and infrastructure, run phishing campaigns, and carry out CE+ assessments.
- Help the sales team by talking with clients to figure out their needs for technical cyber security services.
- Make sure reports are checked for technical accuracy.
- Help your teammates by sharing your experience and knowledge. This includes mentoring and supporting less experienced team members.

Cyber security is an immense industry, and it's unlikely that you'll ever truly stop learning about the many aspects or skills needed to master the domain. The bootcamp will introduce a number of important aspects of the domain, and aims to give you enough of a taste to decide whether cyber security is something you want to continue upskilling in. Although you probably don't currently have the requirements listed in the job specifications above, as this bootcamp progresses, you will begin to feel increasingly confident about where your strengths are and which areas you may need to develop further as you mature as a cyber security professional.

Take note

In the following practical task, you will answer questions related to data breaches and social engineering via email.

Practical task

Imagine this scenario:

You started working at an online consultancy several months ago. You've noticed that the business has a problem with ongoing security breaches. You also noticed that:

- Some staff members are using their personal computers at the office, while others prefer to work from coffee shops/cafes.
- There is no on-site IT technician.
- One of your colleagues was fired because they clicked a link in a phishing email; now everyone is nervous about interacting with their company email account.

Write your own principles-based governance security framework that aims to address and mitigate some of the security problems in your online business, as noted above.

Here are a few examples of frameworks to inspire you:

- **GDPR**
- **NIST**
- **IoTSF IoT Security Assurance Framework Release 3.0**

Save and submit your answer in a .txt file titled **principlesSecurity.txt**.

- Your submission should include five principles.
- Your submission should **not** exceed 400 words.

Important: Be sure to upload all files required for the task submission inside your task folder and then click "Request review" on your dashboard.

Share your thoughts

Please take some time to complete this short feedback **form** to help us ensure we provide you with the best possible learning experience.

Reference list

Belcic, I. (2023, August 25). *What is malware and how to protect against malware attacks?* Avast. **https://www.avast.com/c-malware**

Nigro, P. (2024, February 9). *Cybersecurity governance: A path to cyber maturity.* TechTarget. **https://www.techtarget.com/searchsecurity/post/Cybersecurity-governance-A-path-to-cyber-maturity**