EC-Council

A CISO's top priorities during COVID -19

Authors:

Tom de Haan
Chief Information Security Officer (CISO),
Drechtsteden, Netherlands.

SK Niamathulla
Product Manager – Content Research,
EC-Council, India.

EC-Council Cyber Research

Abstract:

A CISO is the security leader of the organization. The role of the CISO is to support the primary business of multiple divisions and operations of an organization from a security point of view. Though from the technical perspective, the key security responsibilities of a CISO revolve around predicting, identifying, protecting, responding to, and recovering from cyber threats, the CISO is also responsible for looking after governance, compliance, audits, risk management, identity and access management, legal and HR, and the enablement of various aspects of business operations. They also have responsibility for the selection, training, and formation of a dedicated team of threat intelligence analysts for analyzing and predicting threats and vulnerabilities.

As the security head of an organization, a CISO also oversees the SOC and network security functions that detect, monitor, and respond to threats and vulnerabilities in the system and its networks. Responding to any network security incidents and protecting the network from cyberattacks is a major responsibility of a CISO. A CISO must also collaborate with the red team to perform penetration tests against the organization's systems and networks and closely monitor the implementation of the disaster recovery and business continuity protocols of the organization.

This paper discusses the role of CISO in creating a secure work from home (WFH) policy for employees as a by-product of COVID-19 pandemic. We also discuss the role of different cybersecurity units involved in facilitating the smooth functioning of operations and various remote working environments.

Keywords: CISO; COVID-19; Information Security Management System; Security Operations.

Contents

Introduction to how COVID-19 is affecting the role of a CISO

A CISO plays a pivotal role in managing both the internal and external security operations of an organization. A CISO is responsible for establishing and maintaining security strategy, enterprise vision, and ensuring information assets and technologies are protected. CISOs traditionally work alongside the Chief Information Officer (CIO) to achieve their target in such critical COVID-19 situations.

The COVID-19 crisis has far-reaching consequences that will have effects on the global economy for years, if not decades, to come. One of the ways the crisis has impacted the world of information security is the CISO is now charged with safeguarding security operations while employees are all suddenly working remotely. This may mean relying extensively on virtual private networks (VPN) and cloud applications (even shadow IT) that has doubled the cause of concern for the security practitioners. This means organizations have had to revise their security policies and find new ways to ensure the integrity of networks and data.

Roles and Key Skills of a CISO

The CISO is the security leader of an organization who understands Information Security Management (ISM) practice areas and can appropriately identify critical assets that required protection. This professional can determine the threat landscape to a reasonable extent, and thus, attempts to create value through security for the organization.

Figure -1: CISO Roles & Responsibilities

The CISO has the responsibility for designing, implementing, and managing security protections and countermeasures based on compliance and risk management. CISOs must have excellent communication skills. These leaders work with other business heads and secure support from the board when required.

The key characteristics of successful CISOs are:

1. Practical and inspirational leadership style
2. Ability to remain calm under pressure
3. Collaborative and result-driven attitude
4. Skilled multi-tasker
5. Robust technology and security knowledge
6. Risk management
7. Strong business acumen

Skills Needed for Successful CISOs

- The responsibilities of a CISO comprise activities that are technical, managerial, and collaborative.
- Non-technical expertise includes conflict management, communication skills, and political skills.
- The importance of these skills is to improve the ability to clear IT security and privacy technical issues in a non-threatening and transparent manner to non-technical leadership is imperative.
- Understanding political relationships between departments
- CISOs use non-technical skills as they seek cooperation from across state government in building a secure environment.
- Determination, drive, ambition, goal orientation, negotiation, listening, retaining, distilling information, writing skills, editorial skills, likability, dedication, honesty, commitment, accountability, success-orientation, positivity, humility, flexibility, patience, deference to others, consensus building, shared authority, letting people excel without being threatened by their prowess, recognize talent, nurture talent, grow talent, and bring out the best in others.
- Interpersonal communication and managerial skills are equally important or even more important than technical expertise for the success of the CISO. These non-technical skills are just as crucial for accomplishing organizational objectives related to cybersecurity.

Organization Structure of CISO

<table>
<tr><th colspan="4">CHIEF INFORMATION SECURITY OFFICER (CISO)</th></tr>
<tr><td colspan="3">Information Security Executive Council</td><td>Deputy CISO</td></tr>
<tr><td colspan="2">Social Engineering & Asset Security</td><td>Security Operations Center</td><td>Emergency Operations & Incident Mgmt</td><td>Program Management</td></tr>
<tr><td>Security Engineering</td><td>Host & Network Security</td><td rowspan="3" colspan="2"></td><td>PMO</td></tr>
<tr><td>Identify & Access Mgmt</td><td>Information Asset Security</td><td>Governance, Risk, & Compliance</td></tr>
<tr><td>Application Security</td><td>Physical Access Control</td><td>Personal & External Relationships</td></tr>
</table>

Figure – 2 Organization Structure of CISO

Information Security Executive Council

Responsible for

a. Information Technology VP
b. Engineering VP
c. Human Resources
d. Legal
e. CFO/COO/CIO
f. Marketing Business Unit VPs

Governance, Risk, and Compliance

Responsible for

a. Conducting Audits
b. Information security plans
c. Information security program
d. Define and implement infosec policies on risk management
e. Risk management process, strategy, and program governance and compliance

Program Management Office

Responsible for

a. Implementing and maintaining the infosec program, plan, and processes
b. Describing infosec security roles and responsibilities
c. Provideing well trained and skilled resources to implement the infosec security program and plans
d. Communication and reporting
e. Evaluating the status of the security program with top managers

Personnel and External Relationships

Responsible for

Personnel Management:

a. Manage skills, knowledge, ability, availability, performance and employment life cycle of the information security team
b. Implement role-based infosec awareness and training programs to improve in advanced technology.

External Relationship Management

a. Manage relationship with stakeholder, 3rd party services (vendors, FBI, the press)

Security Operations Center (SOC)

Responsible for

a. Detecting and responding to security incidents using an advance technology solution
b. Monitoring users, systems, and applications
c. SIEM Engineers identify, and repel threats

Emergency Operations and Incident Management

Responsible for

a. Incident management
b. Business continuity plans
c. IT Disaster recovery test
d. Root cause analysis
e. Investigation reports

Security Engineering

Responsible for

a. Maintaining Confidentiality, Integrity, and Availability requirements for security architecture
b. Developing secure lifecycle for security architecture
c. Maintaining the report on development and acquisition life cycles of certification and accreditation
d. Performing certification and accreditation before releasing new systems to production

Identity and Access Management

Responsible for

Maintain identities and access controls based on characters. Like

a. Passwords
b. PINs
c. Digital signatures
d. Smart cards
e. Biometrics, etc.

Software and Applications Security

Responsible for

a. Maintaining software and application inventories and application controls
b. Applying changes on software applications
c. Managing configurations for advance software and applications change management
d. IAW security requirements configuration to protect software and applications

Information Asset Security

Responsible for

a. Essential assets
b. Information Asset Inventories
c. Maintaining information asset inventories Information Asset Controls
d. Maintaining necessary controls to protect information and vital assets IAW security requirements

Physical Access Control

Responsible for

a. Implement access controls for assets

b. Access to hosts

c. Access to networks

Host and Network Security

Responsible for

Host and Network Inventories

a. Develop and maintain network, hardware, system, and wired and wireless mobile device inventories Host and Network Control

b. Protect and maintain networks, hardware, systems, and mobile devices IAW security requirements Network Controls (IDS/IPS, etc.)

c. Protect the Internet perimeter IAW security requirements (firewalls, VPNs, etc.) Configuration Management

d. Manage configurations for wired and wireless networks hardware, systems, and mobile devices change management

Five CISO Priorities for dealing with COVID-19

The priorities of a CISO dealing with the challenges of COVID-19 vary depending upon the company and industry. According to the present scenario in the world under COVID-19 – CISOs must have to focus on five areas/functions:

CISO's Responsibilities under Security Operations

CISO Function	Department	Subfunction	Activities	IS Policy
Predict	Threat Intelligence	Internal and external threat intelligence	Analyze data from their own networks (INT) and a variety of sources outside the organization (EXT)	Information Exchange & Threat Intelligence program
Protect	Application Security / Infrastructure security	Configuration Management	Manage configurations for infrastructure, software and applications	Configuration and change management
Detect	SOC	Malicious code management and protection against viruses	Detect, Analyze and mitigate viruses and malicious code	Protect against viruses and malicious code
Respond, Recover	Emergency operation and incident command center	Incident management and response	Detect, examine, analyze, respond to, and recover from suspicious events and security incidents	Security Incident Management
Educate and manage risk	PMO	Information Security Program	Develop infosec plans and implement. Maintain an information security program	Information Security plan

We know the source like policies and procedures, frameworks, standards, and code of practices, which expanded the definition and scope of each specific topic to one of the five functions: Predict, Protect, Monitor/Detect, Recovery & Respond, and Educate & Manage Risk. Each source topic of the five functions was expressed as subfunctions.

With the current pandemic of COVID-19 causing a global health crisis, many organizations and its employees are working remotely from their home places to maintain the business process continuity. But malicious actors are not hesitating to take advantage of this situation to gain benefits. Hence, the responsibilities of IT security engineers, and especially that of CISO's have increased. In these unpredictable times, where things will not go back to normal any soon, the CISO's must determine and configure the applications to be accessible through remote access. Generally, the primary roles and responsibilities of CISO could be classified as the following:

Predicting Threats

The CISO must work with the threat intelligence team to understand the security posture of the organization and utilize strategic intelligence to its full capacity.

What is Threat Intelligence?

Cyber Threat Intelligence (CTI) could also be stated as a group of informed decisions that helps to illuminate the risk landscape instead of advocating a specific solution. CTI supports different activities, namely security operations, incident response, vulnerability and risk management, risk analysis, and fraud prevention. Depending on the intended actions, the sources of CTI may differ.

The discipline of cyber threat intelligence (CTI) focuses on providing actionable information on adversaries. It provides added insight into cyber risks: how and why an organization may get attacked and what could be its impact. You may need an analyst who has the complete knowledge of detecting possible risks and must be able to explain the executives and other departments, the effects of vulnerabilities upon the organization's reputation and financial standing.

As a part of the responsibilities, a CTI analyst may be required to hear the internal security needs and trends, but an even more valuable part is to keep ear to the ground and being aware of the organization-wide trends and risks. The CTI analyst's role reaches to a depth beyond how you might traditionally view an analyst because they are especially skilled in both the technical aspects and observing and identifying the trends that otherwise go unnoticed.

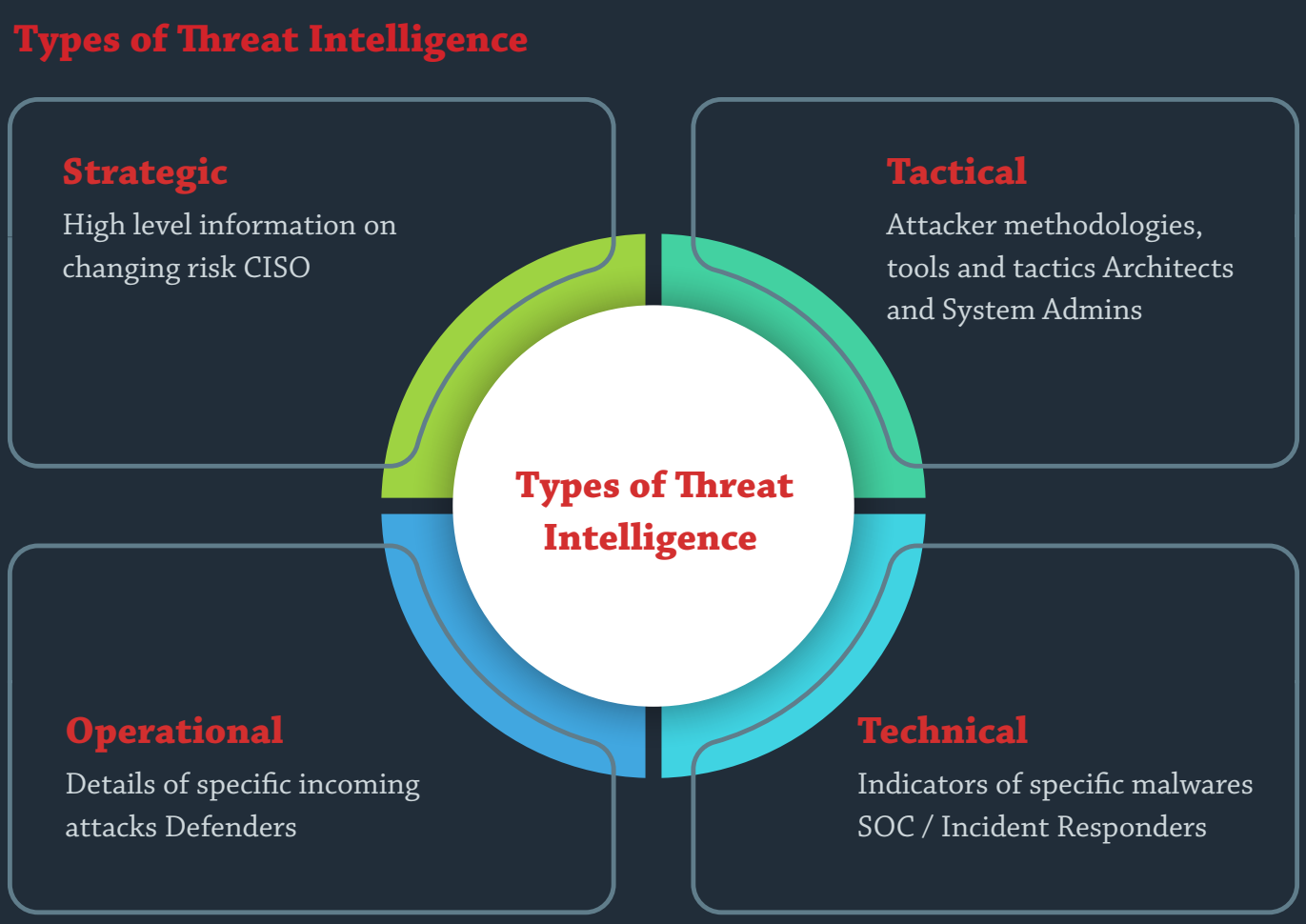


Figure – 3: Types of Threat Intelligence

Threat Intelligence During COVID-19 Outbreak

During the uncertain times of a pandemic where digital burdens have drastically shifted and with the organizations that were unprepared for such scenarios are struggling to maintain the digital security infrastructure. Meanwhile, hackers have found malware and phishing campaigns as the easiest ways to get through the defenses.

Information like campaign structure, domains with indicators of compromise (IOC), and their infrastructure are useful in generating intelligence.

Attackers are designing applications to exploit the public's interest in tracking coronavirus-related statistics such as infections, deaths, and transmissions. These applications plant malware into users' device with the objective to get essential information like personal data, passwords etc.

For example, a malicious website coined as "Coronavirusapp(dot)site" was registered as a domain on March 8th, and claimed to have a real-time Coronavirus outbreak tracker available via an app download. It supposedly at the beginning contained an iframe sourcing directly from infection2020[dot]com (a website from an independent developer for tracking US-based COVID-19 news) and a small banner above that encouraged the installation of its malicious application for real-time updates [1].

IT and cybersecurity experts have successfully obtained a password key for victims of COVIDLock Android ransomware, which comes disguised as an application that superficially claimed to help track cases of the coronavirus, but actually locks users' handhold devices and demands a ransom in order to restore access.

A Domain Tools analysis further revealed that the malware comes with a persistence mechanism for even surviving reboots, and requests access to the permission BIND_DEVICE_ADMIN so it can operate with administrative privileges and take close to full control of the device. In a tricky maneuver, the app says the permission is needed to enable "Accessibility mode" in order to monitor virus stats and also receive alerts of any COVID-19 patients near the user's location [1].

Thus, Cyber Threat Intelligence plays a vital in minimizing cyber risks.

Identify Threats

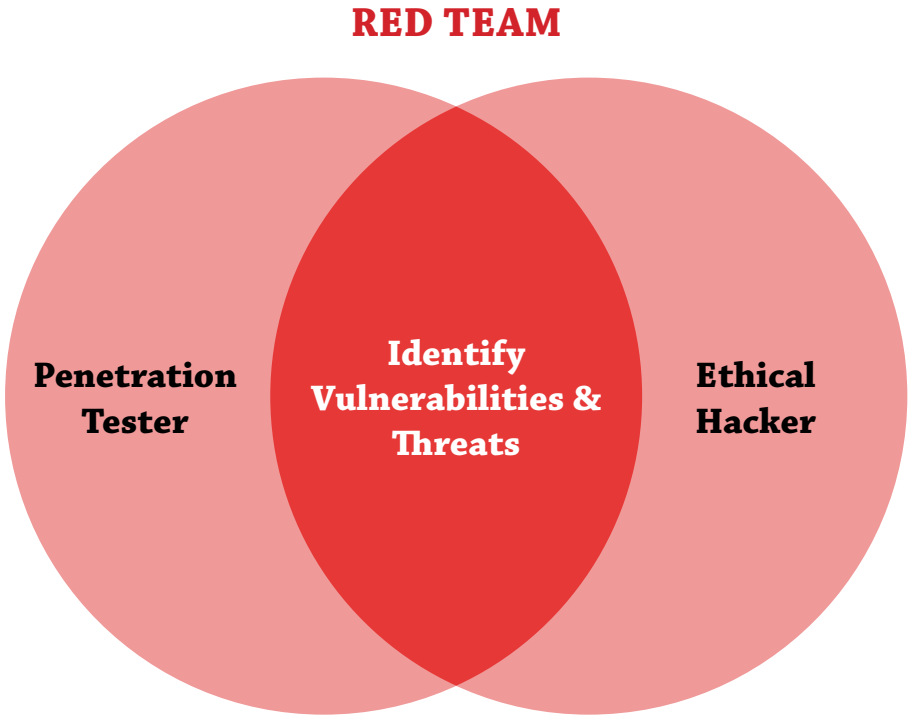
Identification of any vulnerability that may pose a threat to the information security of an organization is the most prominent responsibility of a CISO. Vulnerability assessment implies the incorporation of tools, guidelines, and services that helps identify, classify, and address vulnerabilities across the organization's cyberinfrastructure. This is possible through employing specialists who are well versed in the domain of cybersecurity along with detection tools which, provides advanced level support required to detect and address the vulnerabilities. The role of a CISO is undisputed and of key importance, as they must both employ dedicated security engineers and tools following the security budget while simultaneously not degrading the quality of the security posture.

Monitor and Detect

Depart.	Subfunctions	Activities
SOC	Intelligence collection and threat management	Collect, analyze, examine, and disposition of information from all threat sources
	Situational awareness and common operating picture	Collect, analyze, and report information in (near) real-time that provides situational awareness and a common operating picture
	Logging	Perform audit logging of users, applications, systems, networks, and access to physical assets
	Monitoring	Monitor users, networks, systems, applications, and access to physical assets (includes IDS, IPS, spam filtering, web filtering)
	Vulnerability management	Scan, analyze, and disposition of vulnerabilities
	Virus and malicious code management	Detect, analyze, and mitigate viruses and malicious code
	Information security help desk	Accept, examine, assign, and disposition of all the reported suspicious events and security incidents
	Incident management and response	Detect, examine, analyze, respond to, and recover from suspicious events and security incidents

Role of Red Team

The red teams are majorly focused on pen testing of different networks and their levels of security programs. The team detects, protects, and mitigates the vulnerabilities of the networks.



Penetration Testers

Penetration testing is a comprehensive method to the complete, integrated, operational, and trusted computing base that consists of hardware, software, and people. The process involves a complete active analysis of the network for any potential vulnerability, including poor or improper system configuration, hardware and software flaws, and operational weaknesses in the process or technical countermeasures.

Ethical Hacking

An ethical hacker is a technically skilled professional who hacks into a system or network to scan for pitfalls or hidden difficulties and the probable targets that a cracker can exploit.

Ethical Hacking ~ Hacking **Ethical Hacking ≠ Cracking**

An ethical hacker plays a vital role in identifying potential threats on a network. An ethical hacker attempts to bypass system security and search for any vulnerabilities that could be exploited by malicious hackers. This information is then utilized by the organization to improve the system security, to mitigate the potential attacks.

Many companies tend to adopt third party assistance in this matter, as it tends to remove the administrative burden for maintenance and costs. But this also comes with an added risk if the vendor itself is not secure, compliant, or does not understand the organization's business requirements. The role of a CISO is to identify and shortlist only those that could provide the desired security specific to the supply chain and augmenting the business process of the organization. Some events also call for the security posture assessment of the vendor, termed as vendor risk management.

With changes in technology, the way cybercriminals break into a network has also changed, making it difficult to identify the threat. A CISO needs to ensure that the team is skilled and well trained.

Protect Information

The protection of information (information security) could be achieved through the mitigation of possible information risks. It involves preventing unauthorized access, use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of an organization's information using various tools and techniques. The role of a CISO is to drive different approach towards information protection accordingly. Though information security involves both tangible and digital information for a CISO to handle, digital information tends to take a default form for information security from the perspective of cybersecurity, which is comparatively more vulnerable to compromise.

- The complete structure of risk mitigation can be achieved through:
- Identification of critical assets
- Identification of potential vulnerabilities
- SIEM & Log Management
- Patching
- Encryption of sensitive data with strict access to authorized users only
- Risk evaluation and addressing through either mitigation, avoidance, acceptance or sharing
- Designing appropriate security controls for information access and risk mitigation
- Monitoring activities and responding according to the intent of the user behind the activity
- Maintaining a backup of all the essential information regularly

Among the major classification of information security, i.e., access control, cryptography, compliance, security backup, etc., the CISO must. Apart from these, CISO is also responsible for overall security posture as vulnerabilities can pose a threat to the data. The use of industry standards on password, antivirus software, firewall, encryption software, legal liability, security awareness, and training, etc., should also be considered as an added responsibility of a CISO.

CISO Activities for the Protect function

Department	Subfunctions	Activities
Security Engineers	Security Requirements	Specify & assign confidentiality, integrity & availability requirement
	Security Architecture	Develop and maintain
	Security lifecycle	Security throughout
	Certification & accreditation	Releasing new systems to production
Identity Management	Identity and access management	Define and manage identities or characters and access controls based on identities
Application Security	Software and application inventories	Develop and maintain software and application inventories
	Software and application controls	OS, applications, DBMS, web-based PCI applications.
	Configuration management	Manage configurations for software and applications
	Change management	Manage changes for software and applications
	Host and network controls	Intrusion prevention & Intrusion detection – Network Defense
	Network perimeter controls	Firewalls, DMZ, network connections, third-party services connectivity, remote access, VPNs
	Configuration management	Manage configurations for network hardware and systems Change management

Response and Recovery of Data

Data recovery after the occurrence of a breach or an incident is the core of the disaster recovery and business continuity plan. The recovery involves a set of guidelines, protocols, tools, software applications, etc., to efficiently function together under the observation of a CISO in the event of a natural or human-induced disaster. Disaster recovery could be considered as a subset of business continuity, and also incorporates the functioning of communication services. The role of a CISO in response and recovery is to not only compile guidelines and policies for disaster recovery but also handle the data backupand its reinstallation.

Data backup involves extensive planning as the utilization of different data is done at different speeds at different levels of the business process. The CISO needs to plan the backup and restructuring of the information database accordingly. Many CISO's today opt cloud storage for the important data and process application as it tends to reduce/share the responsibility with the cloud vendors. As a response to the breach or incidents, the role of CISO's provides authority over the investigation and forensics to know the indicators of compromise and develop a corresponding security defense. Also, the CISO is responsible for the compliance and regulatory aspects of data security and needs to steer through the crisis with minimal damage to the information and financial losses to the organization.

The CISO must maintain balanced coordination between the network security team (first responder to network security incidents) and the incident handling/response team.

Recover: The CISO must recognize that strategies around disaster recovery and business continuity play a vital role in restoring normal business operations.

Disaster Recovery plan:

Disaster recovery starts with a list of all assets such as (a) computers (b) networks (c) servers and many more, and it is proposed to identify them using names or numbers uniquely.

"Don't wait for a disaster to happen – implement a disaster recovery plan now."

Every organization should prepare a list of all contacts, including your partners and reputed global service providers like EC-Council Global Service (EGS), to prevent sudden disasters where EGS plays a vital role in providing disaster recovery services globally [2]. EGS offers five services that align with the NIST cybersecurity framework - identify, protect, detect, respond, and disaster recovery, which is further classified into 20 sub-services that help an organization prevent and recover from different cyber disasters.

Further, these organizations should also document IP addresses, usernames, and passwords of servers. With the support of EGS, every organization should follow a few basic and essential steps for disaster recovery:

a. The data center should be accessed only by authorized persons.

b. Every organization's data center should be equipped with a humidity sensor, a surveillance camera, a temperature sensor, a smoke detector, and so on.

Department	Sub-functions	Activities
Emergency operations and incident command centers	Incident Management and Response	Detect, examine, analyze, respond to, and recover from suspicious events and security incidents
	Business continuity	Plan for business continuity (BC)
	IT Disaster Recovery	Plan for disaster recovery (DR)
	Test Response plans	Test BC, DR, and incident management plans
	Investigations	Forensic analysis and investigation with law enforcement

Educate and Manage Risk

Educate and manage risk to make sure that every organization's employees, policies, procedures, compliances, practices, relationships, and advanced technologies provide continuing management, performance measurement, and programs improvement for all the cybersecurity activities.

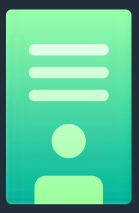
Department	Sub-functions	Activities
Project Mgmt. Officer (PMO)	Cybersecurity or infosec programs	Developing the programs and providing adequate training to implement the infosec security programs
Governance, risk and compliance	Infosec program	Implement infosec policies
	Risk Management	Risk management strategies and process
	Governance and compliance	Monitors legal, regulatory, policy, standards, and security requirements and audits
Personal & 3rd party relationships	External relationships	Relationships with vendors and stakeholders (FBI, press, etc)
	Personal management	Employment lifecycle and performance of the employees

COVID-19 and 5 Pillars of CISO Security

To battle against the COVD-19 challenges, a COVID- 19 CISO Security checklist has been designed for CISOs to implement in their organizations. The list has five pillars explained below:







works	Cyber Security Team	Awareness and Training Outsourcing	Security Reports	IT systems and net

Review IT Systems and Networks	Based on the coronavirus/COVID-19 analysis, the threat landscape has become more vulnerable and prone to cyber-attacks. The crucial aspect of a network or server lies in the amount of data stored in it. Hence, during any disaster or natural hazard, it is imperative to check the list of IT security products such as anti-Malware, anti-Virus programs are upgraded, installed, and configured (hardened) accordingly.
Certified Cyber Security Team	To handle the past and the present COVID-19 situation's ongoing security operations, an organization should ensure to have a dedicated team of security experts who can address and implement revised security procedures and stay consistent with the organization's IT strategy to protect the confidentiality, integrity, and availability of information.
Cybersecurity Awareness and Training	Though professionals working in a remote environment are abreast of specific security measures and policies, there might be fewer chances of them becoming victims of social engineering acts. In this regard, security awareness and training are the need of the situation to ensure your workforce is capable of defending vulnerabilities and able to respond promptly. The board should have frequent notifications and communications, informing the employees about the latest changes in IT.

Global Services (Outsourcing)	Many organizations rely on third-party service providers (Identify, Protect, Detect, Respond, Recover) for assessing and protecting their IT infrastructures. Their in-house security practitioners may not be technically skilled to handle massive disasters, such as COVID-19, promptly. And looking at the present thick and inflexible time, companies should consider hiring an MSSP (Managed Security Service Providers), because they operate 24/7 to provide security monitoring and threat detection analysis of systems and devices.
Periodic Security Reports	A periodic report consisting of the present security posture of an organization must be presented, to the management, specifying the existing security trends with a thorough analysis if an attack existed and the status of the implications.

Role of CISO in creating a secure work from home (WFH) policy for all employees

Since the outbreak of COVID-19 in the last three months and working professionals remotely connecting, have increased the risk of cyberattacks on systems and home networks. Cybercriminals are using this as an opportunity to attack by sending phishing emails, social engineering, and more. This switch has created havoc between employers and employees.

Due to this pandemic, CISOs are facing much pressure on their shoulders, addressing security and compliance challenges.

However, due to this sudden organizational change CISOs must immediately investigate the unforeseen threats –

Below are some best practices set by CISO, that every organization should adhere to

- Ensure that the teams are aware and trained in detecting any malicious activity and report the security team immediately.
- Since the significant attacks are coming via phishing, social engineering, malware, the professionals should be educated about these attacks and be cautious operating with due diligence and not revealing confidential data to anyone.
- Since the employees are operating from multiple locations using various devices and different networks, they should be regularly monitored.
- Ensure timely updates on what the organization is doing to combat COVID-19 in terms of protecting and securing the data.

References:

1. https://www.scmagazine.com/home/security-news/news-archive/coronavirus/password-found-to-rescue-victims-of-malicious-covid-19-tracker-app/
2. https://egs.eccouncil.org/services/business-continuity-management-disaster-recovery-plan/
3. https://blog.eccouncil.org/how-to-create-an-effective-disaster-recovery-plan-in-5-steps/
4. https://www.scmagazine.com/home/security-news/news-archive/coronavirus/password-found-to-rescue-victims-of-malicious-covid-19-tracker-app/
5. https://www.csoonline.com/article/3534521/3-ways-covid-19-is-changing-ciso-priorities.html
6. https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2019/new-forbes-insights-report.html
7. https://resources.infosecinstitute.com/management-guide-for-cisos-responsibilities-strategies-and-best-practices/#gref
8. https://blog.eccouncil.org/wireless-pen-testing-to-protect-wireless-networks-using-wpa2-over-advanced-wpa3/

Frequently asked questions

What is the CCISO Certification?

The Certified CISO (CCISO) is an exclusive program designed to produce top-level information security leaders by focusing on both technical skills and information security management strategies in accordance with the executive management goals.

Read more: https://blog.eccouncil.org/building-competent-cisos-through-the-certified-chief-information-security-officer-program/

How long does it take to become a CISO?

Chief Information Security Officer (CISO) role requires 8-10 years of progressive cybersecurity experience. Jobs in programming, information security, risk management, and government are all great foundations for CISO positions..

Read more: https://ciso.eccouncil.org/webinars/

How do I become a CISO?

1. CISO education requirements generally include earning a bachelor's degree
2. Get cybersecurity experience. On average, the CISO role requires 8-10 years of progressive IT security experience.
3. Complete IT Security certification and training

Read more: https://blog.eccouncil.org/creating-cybersecurity-leaders-for-2020-and-beyond-ec-councils-certified-chief-information-security-officer/

EC-Council