I'm not a robot

Cybersecurity is becoming a critical concern as various industries depend on digital infrastructure. To protect sensitive information from cyber threats, governments worldwide have introduced cybersecurity regulations for specific sectors that help secure digital ecosystems and prevent cyber attacks.Understanding the specific regulations for your organization’s industry is essential for risk management. This blog covers a comprehensive overview of cybersecurity regulations across various sectors and their implications for organizations, providing valuable insights into compliance requirements and best practices for securing digital ecosystems.Secure your organization’s digital assets with UpGuard >Cybersecurity Regulations vs Cybersecurity FrameworksCybersecurity regulations and frameworks are two standard terms in the cybersecurity industry. While they share a common goal of enhancing cybersecurity practices, they differ distinctly.Cybersecurity regulations are rules legally enforced by government authorities or regulatory bodies. Examples include HIPAA, PCI DSS, GDPR, etc. These rules are specific to each industry and require organizations to follow particular cybersecurity standards and practices. Organizations not complying with these compliance regulations may face penalties, fines, or legal action. Key regulatory requirements include:Mandatory Compliance: Organizations subject to cybersecurity regulations have a legal obligation to meet specific cybersecurity requirements, and non-compliance can result in severe consequences.Enforceability: Regulatory bodies possess the power to ensure cybersecurity compliance with regulations by conducting audits, inspections, and imposing penalties.Industry Specific: Specific regulatory compliance is tailored to individual industries due to unique risks and needs.Prescriptive: Regulations typically outline specific guidelines, standards, and security controls that organizations must adhere to.On the other hand, cybersecurity frameworks are a set of voluntary guidelines and best practices developed by cybersecurity experts and organizations to assist organizations in enhancing their cybersecurity posture. Popular cybersecurity frameworks include the National Institute of Standards and Technology (NIST), CIS Controls, and the ISO/IEC 27001 standard. Many organizations voluntarily adopt frameworks to demonstrate their commitment to cybersecurity and strengthen security measures. Key characteristics of cybersecurity frameworks include:Voluntary Adoption: Organizations can choose to implement cybersecurity frameworks based on their specific needs and risk profiles.Flexibility: Frameworks provide a flexible approach to cybersecurity, allowing organizations to tailor their security measures to their unique circumstances.Guidance and Best Practices: Frameworks offer guidance, best practices, and recommendations to help organizations establish effective cybersecurity programs.Financial ServicesThe financial services sector is a crucial part of the global economy, as it deals with sensitive financial information daily. Due to the high level of risk and the constant threat of cyberattacks, ransomware, phishing, etc., financial institutions must comply with rigorous cybersecurity regulations. Below are the main cybersecurity regulations that apply to the financial services industry and insights into their requirements and implications for various players.Gramm-Leach-Bliley Act (GLBA)The GLBA, also known as the Gramm-Leach-Bliley Act, is a critical legislation safeguarding consumers' financial privacy. It was enacted in 1999 and applies to financial institutions such as banks, credit unions, and securities firms. Its main aim is to enforce strict security measures that protect customers' non-public personal information (NPI). Financial institutions must prioritize protecting customer data to avoid fines and legal consequences and maintain trust.Key components of the GLBA include:Privacy Notices: Financial institutions must provide annual privacy notices to customers, outlining the institution's information-sharing practices.Safeguarding NPI: The GLBA mandates that institutions develop security programs to protect NPI from unauthorized access or disclosure (i.e., access control, multi-factor authentication, etc.)Third-party Oversight: Financial institutions must assess and monitor third parties' cybersecurity practices and security policies with NPI access.Payment Card Industry Data Security Standard (PCI DSS)Organizations or businesses that handle payment card transactions must comply with the Payment Card Industry Data Security Standard (PCI DSS). The payment card industry established this set of security standards to protect cardholder data, a critical piece of sensitive information. PCI DSS is not a government regulation but is critical for businesses that process credit card transactions, as non-compliance can result in severe penalties, loss of customer trust, and even potentially devastating data breaches.Key components of the PCI DSS include:Data Encryption: PCI DSS requires the encryption of cardholder data during transmission and storage.Regular Audits: Organizations must undergo regular security assessments and audits to maintain compliance.Network Security: PCI DSS provides guidelines for securing network infrastructure to prevent data breaches.Sarbanes-Oxley Act (SOX)The Sarbanes-Oxley Act, or SOX, was created to respond to the many corporate accounting scandals in the early 2000s, focusing primarily on financial reporting and corporate governance. However, it also has implications for cybersecurity in financial institutions, specifically regarding the accuracy and reliability of financial data. Financial institutions, including publicly traded companies, must ensure compliance with SOX to maintain transparency and prevent fraudulent financial practices. Non-compliance can result in various consequences, ranging from legal issues to financial fees.Key components of SOX include:Internal Controls: SOX mandates that companies utilize internal controls to protect the accuracy and integrity of financial reports.Data Retention: The Act includes provisions for securing financial records and electronic communications.Whistleblower Protection: SOX protects whistleblowers who report corporate misconduct, including cybersecurity violations.HealthcareThe healthcare industry is responsible for safeguarding sensitive and personal patient information. As healthcare providers, insurers, and organizations rely more on digital systems for patient care and data management, it is crucial to protect patient information from cyber threats. It’s also one of the most heavily targeted sectors by cybercriminals. Below are the most common cybersecurity regulations that govern the healthcare sector, including their requirements and outcomes for safeguarding patient data.Health Insurance Portability and Accountability Act (HIPAA)The Health Insurance Portability and Accountability Act, or HIPAA, is a crucial regulation in healthcare that came into effect in 1996. Its primary goal is safeguarding patients' Protected Health Information (PHI) privacy and security. Failure to comply with HIPAA can result in severe consequences, including significant monetary fines and criminal charges. To avoid such penalties, healthcare organizations must prioritize patient data security.Key components of HIPAA include:Privacy Rule: The HIPAA Privacy Rule dictates how healthcare organizations can use and disclose PHI and grants patients certain rights over their health data.Security Rule: The HIPAA Security Rule requires administrative, physical, and technical security measures to protect the confidentiality, integrity, and availability of electronic PHI.Breach Notification: HIPAA requires healthcare organizations to report breaches of unsecured ePHI to affected individuals, the Department of Health and Human Services, and—in some cases—the media.Health Information Technology for Economic and Clinical Health Act (HITECH)The HITECH Act, short for the Health Information Technology for Economic and Clinical Health Act, is a law passed in 2009 that complements HIPAA by emphasizing electronic health records (EHRs) and the advancement of healthcare information technology. This act extends HIPAA's privacy and security requirements and encourages healthcare organizations to invest in strong cybersecurity measures. Its focus on promoting secure EHR adoption and stricter enforcement of HIPAA requirements is crucial for advancing the healthcare industry's security.Key components of HITECH include:Meaningful Use: HITECH encourages the adoption and "meaningful use" of EHRs, promoting secure and interoperable health information exchange.Enforcement: The Act strengthens HIPAA enforcement, increasing penalties for violations and expanding the scope of enforcement to include business associates.Breach Notifications: Like HIPAA, HITECH requires healthcare organizations to notify affected individuals and HHS in case of a data breach involving unsecured PHI.Government and the Public SectorThe government and public sector have a unique and crucial role in cybersecurity. They hold a significant amount of sensitive data, including citizens' personal information and national security-related data. As cyber threats continue to evolve, it has become essential to have regulations governing cybersecurity in this sector. Below are the key cybersecurity regulations that shape the government and public sector's approach to safeguarding critical information and infrastructure.Federal Information Security Management Act (FISMA)The Federal Information Security Management Act (FISMA) was enacted in 2002 and is a critical component of federal cybersecurity regulation. It defines the guidelines for safeguarding federal information systems and data. Adhering to FISMA is crucial for federal agencies to uphold the security and integrity of government data and infrastructure. Failure to comply with FISMA's requirements can result in a breach of national security and data breaches.Key components of FISMA include:Risk Management: FISMA emphasizes a risk-based approach to information security, requiring federal agencies to identify, assess, and mitigate cybersecurity risks.Continuous Monitoring: The Act mandates continuous monitoring of information systems and the development of security plans and policies.Reporting Requirements: FISMA requires federal agencies to report security incidents and compliance status to the Office of Management and Budget (OMB) and Congress.Homeland Security Act of 2002In 2002, the Homeland Security Act created the Department of Homeland Security (DHS) to safeguard the country's vital infrastructure from potential cybersecurity threats. The Act stresses the significance of cooperation and coordination between government organizations and private entities to protect against cyber attacks that could harm critical infrastructure.Key components of the Homeland Security Act of 2002 include:DHS Authority: The Act grants the DHS authority to oversee the security of critical infrastructure sectors and develop strategies for mitigating cybersecurity risks.Information Sharing: It encourages information sharing between government agencies (like the Department of Defense), private-sector partners, and critical infrastructure owners and operators.Emergency Response: The Act outlines procedures and incident response plans for cybersecurity incidents that may have national security implications.General Data Protection Regulation (GDPR)While the General Data Protection Regulation (GDPR) is a European regulation, its reach extends beyond the EU and affects any organization that processes the personal data of EU residents. The GDPR, which came into effect in 2018, places stringent data protection and privacy requirements on organizations across various sectors. Non-compliance with the GDPR can result in substantial fines, making it essential for organizations with global operations to align their cybersecurity practices with GDPR principles.Key components of the GDPR for healthcare organizations include:Extraterritorial Scope: The GDPR applies to organizations worldwide if they process the personal data of EU residents.Data Protection Principles: The GDPR emphasizes data protection principles, including the lawful processing of personal data, data minimization, and data subject rights.Data Breach Notification: The GDPR requires the notification of data breaches to the relevant supervisory authority and, in some cases, data subjects.Cybersecurity Information Sharing Act (CISA)The Cybersecurity Information Sharing Act (CISA), introduced in 2015, focuses on improving the communication of cybersecurity threat information between the private sector and the federal government. CISA promotes the exchange of crucial cybersecurity threat intelligence, which enhances the collective ability to identify and respond to cyber threats effectively.Key components of CISA include:Information Sharing: CISA encourages organizations to share cyber threat information and defensive measures with the government and other private entities.Liability Protections: The Act protects organizations that share threat information in good faith.Privacy Protections: CISA includes provisions to protect privacy and civil liberties, ensuring that personally identifiable information (PII) is appropriately handled.Retail and E-CommerceThe retail and e-commerce industries have undergone significant changes in recent years. More consumers now prefer to shop online, which has led to a greater emphasis on cybersecurity. These industries handle significant swaths of customer data, such as payment information and personal details, and rely heavily on the supply chain. Therefore, complying with cybersecurity regulations to protect this information in a digital marketplace is crucial. Below are the primary cybersecurity regulations that affect retail and e-commerce sectors, along with the requirements and implications of protecting customer data.California Consumer Privacy Act (CCPA)The CCPA, or California Consumer Privacy Act, is a significant step toward regulating consumer data privacy. It was enacted in 2018 and implemented in 2020, giving California residents greater control over their personal information. The CCPA imposes new responsibilities on businesses operating in California and has wide coverage, not limited to California-based companies. It applies to any business that processes personal information, making it an important regulation for e-commerce businesses.Key components of the CCPA include:Consumer Rights: The CCPA gives California residents the right to access, delete, and opt out of the sale of their personal information.Data Handling Requirements: Businesses must disclose their data collection and sharing practices and implement data protection measures.Non-Discrimination: The CCPA prohibits businesses from discriminating against consumers who exercise their privacy rights.Children’s Online Privacy Protection Act (COPPA)The Children's Online Privacy Protection Act (COPPA) was enacted in 1998 and amended in 2013 to safeguard the online privacy of children under 13. COPPA imposes certain obligations on websites and online services collecting children's data. To avoid penalties for mishandling children's data, e-commerce platforms and websites catering to children or with child-oriented content must comply with COPPA.Key components of COPPA include:Parental Consent: COPPA requires parental consent to collect personal information from children.Privacy Notices: Websites must provide clear and concise privacy notices outlining data collection practices.Data Security: COPPA mandates reasonable data security practices to protect children's information.Fair and Accurate Credit Transactions Act (FACTA)The Fair and Accurate Credit Transactions Act (FACTA) is a law that seeks to safeguard consumer credit information and payment card data. Although FACTA mainly targets credit reporting, it has cybersecurity implications for retailers and businesses that engage in payment card transactions. Retailers and businesses involved in payment card transactions must comply with FACTA regulations to prevent identity theft and financial fraud.Key components of FACTA include:Red Flag Rules: FACTA's Red Flag Rules require businesses to implement identity theft prevention programs.Disposal of Customer Information: The Act mandates secure disposal of customer information, including payment card data.Truncation of Card Numbers: FACTA prohibits printing more than the last five digits of a credit card number on receipts.Technology and TelecommunicationsThe technology and telecommunications sectors lead innovation, providing advanced solutions and connectivity for the digital age. However, cybercriminals often target these industries, so various cybersecurity regulations have been implemented to ensure the security of technology and telecommunications networks and safeguard sensitive data. Below are the key cybersecurity regulations shaping the technology and telecommunications landscape, providing insights into their requirements and impacts on protecting critical information and infrastructure.The Electronic Communications Privacy Act (ECPA)The Electronic Communications Privacy Act (ECPA) is an important law that deals with electronic communication privacy. It was first enacted in 1986 and has been amended several times. The ECPA sets legal standards for accessing and intercepting electronic communications and records that have been stored. This law is important because it helps to balance individual privacy rights with legitimate law enforcement activities. As a result, it is a crucial regulation for technology and telecommunications providers.Key Components of the ECPA include:Warrant Requirements: The ECPA outlines the circumstances under which law enforcement agencies can access email communications and other electronic records, often requiring a warrant.Wiretap Provisions: The Act governs wiretapping of electronic communications, with specific rules for interception of phone conversations and electronic communications.Stored Communications: The ECPA defines the conditions under which government agencies can access stored electronic communications, such as emails and documents.The Computer Fraud and Abuse Act (CFAA)The Computer Fraud and Abuse Act (CFAA) is a federal law that targets computer-related crimes and unauthorized access to computer systems. It was enacted in 1986 and has been amended multiple times since then. The CFAA is a crucial piece of legislation that helps in the fight against cybercrime. It is vital in deterring cybercriminals and protecting technology and telecommunications systems from unauthorized intrusion.Key components of the CFAA include:Unauthorized Access: The CFAA prohibits unauthorized access to computer systems, networks, and data.Fraudulent Activities: The Act addresses various forms of cyber fraud, including identity theft and unauthorized access with malicious intent.Penalties: The CFAA outlines penalties for those found guilty of cybercrimes, which may include fines and imprisonment.Telecommunications Act of 1996The Telecommunications Act of 1996 is a law that has significantly impacted the telecommunications industry in the United States. Its main goal is to encourage competition and regulate telecommunications services. However, it also has cybersecurity implications that relate to safeguarding telecommunications networks. The Telecommunications Act has played a vital role in shaping the current telecommunications landscape and remains a critical influence on how security is addressed within the sector.Key components of the Telecommunications Act of 1996 include:Competition: The Act encourages competition in the telecommunications sector, which can lead to improved security postures.Emergency Services: It mandates providing emergency services via telecommunications networks, necessitating robust network security.Access and Interconnection: The Act addresses network access and interconnection issues, which have cybersecurity implications regarding network integrity and protection.Stay Compliant with Cybersecurity Regulations using UpGuardUpGuard is an attack surface monitoring solution that supports a variety of cybersecurity regulations both internally and throughout the vendor network. The analytics from these efforts can then create a risk treatment plan to keep stakeholders and interested parties continuously informed about your organization's security posture.Our products, Breach Risk and Vendor Risk, can help your organization achieve compliance with various cybersecurity regulations. Check out their features below!UpGuard BreachSight: Attack Surface ManagementData leak detection: Protect your brand, intellectual property, and customer data with timely detection of data leaks and avoid sensitive data breachesContinuous monitoring: Get real-time information and manage exposures, including domains, IPs, and employee credentialsAttack surface reduction: Reduce your attack surface by discovering exploitable vulnerabilities and domains at risk of typosquattingShared security profile: Eliminate having to answer security questionnaires by creating a Trust PageWorkflows and waivers: Simplify and accelerate how you remediate issues, waive risks, and respond to security queriesReporting and insights: Access tailor-made reports for different stakeholders and view information about your external attack surfaceUpGuard Vendor Risk: Third-Party Risk ManagementSecurity questionnaires: Automate security questionnaires with workflows to get deeper insights into your vendors’ security and supplier relationshipsSecurity ratings: Instantly understand your vendors' security posture with our data-driven, objective, and dynamic security ratingsRisk assessments: Let us guide you each step of the way, from gathering evidence, assessing risks, and requesting remediationMonitor vendor risk: Monitor your vendors daily and view the details to understand what risks impact their security posture throughout their lifecycle.Reporting and insights: UpGuard’s Reports Library makes it easier and faster for you to access tailor-made reports for different stakeholdersManaged third-party risks: Let our expert analysts manage your third-party risk management program and allocate your security resources The Software Security Requirements Checklist is a comprehensive tool that helps organizations identify and quantify their software security needs. It covers the full range of security topics, from application security to network security and includes detailed questions about compliance, risk management, and access control. It can also help organizations identify gaps in their existing security measures and provide guidance for improving them. The checklist is designed to help organizations create a comprehensive plan for software security that meets industry standards and best practices. A cybersecurity checklist is important since cybersecurity investments can be a complicated process. An organization must first identify vulnerable assets, determine how vulnerable they are, and allocate sufficient budgets needed to enhance their security. In any cybersecurity program, companies should, at the very least, include the following: Developing a holistic program means covering all IT assets and information systems. For organizations with vast software, hardware, or network products, it can be challenging to develop an all-rounded cybersecurity program. This necessitates the use of a cybersecurity checklist. A cybersecurity checklist lists items that must be protected. It identifies and documents a set of cybersecurity procedures, standards, policies, and controls. The following sections discuss important items that must be included in a cybersecurity checklist. All organizations should identify the best security practices when accessing or handling sensitive data and critical information systems. The following three items are essential to maintaining a useful cybersecurity checklist. Documented policies list the security guidelines and obligations of employees when interacting with company systems or networks. The policies enable an organization to ensure employees, third parties, or managed service providers observe minimum but mandatory security measures. Common policies to include in a cybersecurity checklist include acceptable use, internet access, email and communication, remote access, BYOD, encryption and privacy, and disaster recovery. A cybersecurity checklist should include an acceptable use policy. Acceptable use consists of various rules that govern the use of an organization’s IT assets or data. The policy is crucial since it prevents system users from participating in practices that can impact the cybersecurity of an organization. All new users, which might be employees, third parties, and contractors, must accept to have read and understood the stipulated rules. This is before being allowed to access company networks and computer systems. By acknowledging to understand the policy, users agree to use information systems according to the organization’s minimum-security recommendations. As such, a business can be assured that user activities will not introduce security risks and threats. The internet has become ingrained in the daily activities of most individuals. People use the internet for research, accessing cloud services, and communicating through emails or social media platforms, among others. However, the same internet can be the downfall of an organization due to various reasons. For instance, cyber actors use the internet to deliver malware. They can place malware on a specific website such that any user who visits it downloads and installs the malware. Such and other attacks executed through the internet are frequent. Therefore, a cybersecurity checklist should include a policy governing internet usage within an organization. Internet access policy contains guidelines regarding how users can access and interact with the internet. For instance, an internet access policy can prohibit users from visiting specific websites, or the frequency with which they can access social media platforms. This can facilitate the adoption of bolstered and strengthened cybersecurity postures. Emails are used for both internal and external communication. All employees in an organization must, therefore, have an email account. Emails are also an attacker’s preferred mode of delivering phishing malware. Hackers send emails in batches to multiple targets hoping that one will click on the links or attachments containing malware. A policy regarding email usage can enable a company to prevent phishing attacks, thus improving the security of its data and systems. Such a policy can include rules requiring employees not to open emails sent by unknown people. Also, it can require that all incoming emails be scanned to detect malicious attachments or links with hidden malware. Additionally, an email and communications policy should require employees to avoid using personal emails when communicating work-related data. Such policies are essential to ensuring organizational security and should, therefore, be included in a cybersecurity checklist. More businesses are adopting cloud technologies. This is to enhance their data collection and processing techniques and to improve employee productivity. Since cloud services are becoming more ingrained in running daily business operations, a cybersecurity checklist must contain a remote access policy. Remote access policies provide the necessary security requirements users should consider when accessing cloud accounts remotely. The cloud permits users to access data and other services from any location and device. This means that they can opt to work remotely outside the office. A remote access policy ensures that they observe secure practices when accessing sensitive information. For instance, the policy can require employees to use a VPN when accessing through a public and insecure internet network. Internet of Things has proliferated in recent years, leading to increased use of internet-enabled devices. The trend has seen most employees prefer using personal devices such as smartwatches, laptops, smartphones, and tablets to accomplish their assigned duties. This results in increased risks since the more the devices in use, the more the number of entry points a hacker can choose from. That notwithstanding, users may be unable to identify vulnerabilities present in their devices. Connecting to a corporate network or accessing data using vulnerable devices threatens their integrity, confidentiality, and availability. A BYOD policy enables an organization to manage the use of personal devices within a work environment, thus alleviating risks that can impact its overall security. A BYOD policy can include requirements such as employees only connecting to the corporate network using devices provided by the organization. A BYOD policy should be updated frequently to ensure it covers all emerging technologies. Including a BYOD policy in a cybersecurity checklist facilitates the secure usage of personal devices, thus protecting an organization from multiple threat sources. Sometimes, cyber adversaries manage to bypass the most secure networks and systems. As such, organizations are not fully guaranteed that their data and classified information are 100% secure. An encryption and privacy policy should hence be a requirement in all processes where users interact with organizational data. The encryption and privacy policy should require users to encrypt all data, whether it is at rest or in transit. Encrypting data provides an additional security layer to the encrypted information if cyber adversaries manage to breach the adopted cyber defenses. Moreover, the policy should include the preferred encryption technique to ascertain that all users use the same level of standard encryption techniques. Encryption should be included in all cybersecurity programs and checklists since it is the simplest method for preserving data integrity, confidentiality, and availability. As previously stated, adopting the most powerful security solutions do not guarantee that an organization is entirely secure. In anticipation of the occurrence of a cyber-attack, businesses should maintain effective disaster recovery policies. A disaster recovery policy contains a set of actions that different users should undertake to recover from an attack. Developing effective disaster recovery policies can facilitate a company’s efforts to contain an attack. Also, by maintaining and continuously updating a disaster recovery policy, a business assigns its employees the roles to complete to ensure a speedy recovery of critical data, networks, or computer systems. The policy further addresses the communication channels to ensure that the involved personnel has seamless communication during the entire time of a disaster recovery process. A disaster recovery policy should, therefore, be at the heart of all cybersecurity checklists. Every business should consider including the use of modern software programs in its cybersecurity checklist. Acquiring up-to-date software is vital to enhancing the security of an organization. This is because modern software programs are developed to be resilient against current risks and attacks. Using legacy operating or software systems introduces various security challenges. They might be containing unaddressed vulnerabilities, or their vendors might have stopped supporting them in releasing security updates and patches. Using current software does not necessarily mean that it is entirely secure. Vulnerabilities emerge all the time, and failing to address them can provide hackers with a playing ground for exploiting the vulnerabilities. As such, a cybersecurity checklist should include a patch management program. Software or hardware vendors release security patches to mitigate vulnerabilities as they occur. Regularly applying security patches can help protect an organization from cyber-attack incidences. More than 90% of the cyber incidences are caused by erroneous user mistakes or cybersecurity ignorance. For example, an employee leaving a computer without locking can result in disastrous data breaches. For this reason, all organizations need to include frequent training and awareness campaigns in their cybersecurity programs. Training and awareness provide employees with skills for securely using organizational systems, data, and networks. It also ensures that they are capable of identifying security risks, managing them, and reporting them to the relevant personnel. In this regard, an employee training program should train employees on how to secure their workstations, emails, cloud accounts, and other types of information systems. Also, a training program should enable employees to understand how they can identify phishing emails and the actions they should undertake once identified. Such measures include marking the sender’s email address as spam, reporting to IT, and alerting other employees of the attempted phishing attacks. There are other training items to be considered when developing an awareness and training program. These should be included to meet a company’s security needs. A practical cybersecurity checklist should contain measures that are specific to network and system users. The standards ensure that an organization remains protected whenever a user accesses the IT assets at his disposal. The following items need to be included in a cybersecurity checklist. This is to ascertain that user behaviors do not impact organizational cybersecurity. Password etiquette refers to what consists of best password management practices. Passwords are often the most used defenses at all levels, and users must ensure that they observe best password practices. An essential password security requirement is users should always create robust passwords. The guidelines to consider include combining different characters such as numbers, alphabetical letters, and special symbols. This is to minimize the possibility of cyber adversaries guessing the passwords. Also, a business should require users to create lengthy passwords. Passwords with 6-10 characters can provide sufficient security. It is also crucial for users to frequently change and update their passwords. A rogue college might access stored passwords and use them for identity theft or other malicious activities. To ensure high password complexity, users should consider using passphrases. These are strings of different words required to access a system. These and other password requirements should be included in a cybersecurity checklist. Work accounts such as email and cloud accounts can be disabled due to various reasons. These reasons can include employees being reassigned to new roles and responsibilities, or if an employee stops working in an organization. Auditing disabled accounts allow a system administrator to identify accounts that are no longer in use. Disabled accounts provide security risks since malicious actors can access them along with all permissions and privileges. As such, they can gain system and data access while posing as legitimate users. An audit of all outdated accounts ensures that those no longer in use are closed and deleted. Including auditing disabled or outdated accounts in a cybersecurity checklist enable a company to close all loopholes that can give adversaries unauthorized access to protected systems and information. Preventing users from sharing the same passwords or work accounts should be a priority for any cybersecurity program or checklist. Allowing users to share work accounts and passwords can result in highly impactful security risks. For example, it can be difficult to trace the user responsible for a security incident if it involves a shared account. Besides, allowing employees to share accounts and passwords encourages insider threats and attacks. Employees participating in malicious activities can deny any accusations, pointing out that they are not the only ones with access to the account in question. Therefore, including the prevention of shared passwords and accounts as an item in a cybersecurity checklist can ensure a company audits all accounts. Subsequently, insider threats can be minimized, thus leading to enhanced cybersecurity. The use of secure websites, when connected to an organization’s network, should be a mandatory item in a cybersecurity checklist. Every business should require employees to only share organizational information or any sensitive data like passwords through secure websites. Secure sites have an HTTPS connection, which means that the connection is encrypted. Encrypted connections allow secure data and information transfer, which is vital to ensuring that its integrity and confidentiality remain intact. Including the use of secure and encrypted websites in a cybersecurity checklist can enable a company to block users from accessing insecure websites. This eliminates instances where cyber incidences are as a result of the information being compromised through vulnerable sites. Such sites have an HTTP connection and as such, lack the necessary encryption schemes. Almost all communication processes are done via email communication. Emails, however, provided the highest risks since they are a preference for delivering malware and viruses for most cyber actors. It is, therefore, essential for an organization to include email security in its cybersecurity checklist. The following are some of the points to consider in email security. Email communication is the most widely used platform for executing phishing attacks and delivering malware. Phishing attacks are where cyber adversaries target multiple users with messages crafted to appeal to their interests. This is to trick them into clicking on a link or attachment that contains hidden malware. To ensure that such malware programs are caught before a user downloads them, businesses need to install tools for filtering all incoming messages. As such, they can detect embedded malware and prevent them from accessing the company’s networks or computer systems. Developing and regularly updating an email policy should be included in a cybersecurity checklist. Emails can still be hacked without the knowledge of an organization, as email security is usually the responsibility of the email service provider. Documenting an email policy identifies the types of information that users are permitted or prohibited from sharing through emails. For example, an email policy can prevent users from sharing passwords, personal data, or financial information through emails. Businesses use their websites for marketing their products and services. They also use emails to interact with customers by responding to inquiries or customer feedback. In some cases, some companies might collect a client’s personal information through their websites. Website security should, therefore, be an essential item in a cybersecurity checklist. There are two main points to consider to realize optimum website security. Companies need to obtain an SSL (Secure Sockets Layer) certification. An SSL-certified website means that it is secure, and it provides end-to-end encryption between a client and a server. By being SSL certified, a user can confidently transmit sensitive information without fearing that it will be intercepted and modified before it reaches the intended target. Moreover, an SSL-certified website not only means that users can access it and securely request or transmit information, but it also builds a company’s reputation. Customers prefer submitting their information through secure sites, and SSL certificate gains their confidence. As such, it is necessary to include SSL certification in a cybersecurity checklist. An organization should only seek the services of a secure web hosting provider. The key attributes to include in a cybersecurity checklist are the provider’s ability to isolate hosting accounts, mechanisms for regularly backing up the website, and the ability to maintain the server logs. Ensuring network security is crucial to any business. Cyber adversaries are always looking for exploitable network vulnerabilities to gain unauthorized access. The following items should be present in a cybersecurity checklist to realize maximum website security. A network should be secured using powerful firewalls. Combining several firewalls can provide enhanced network security. Protecting networks using a firewall facilitates the development of filtering rules in accordance with an organization’s security requirements. The rules are for filtering out incoming malicious connections that can affect the security of the network. Maintain password security ensures only users with the correct permissions can connect to the network. A business should hence apply password security in its Wi-Fi routers to ensure only employees can access internal networks. To minimize the risk of a malicious user accessing the corporate network, a business should provide guests with a separate Wi-Fi network. Network segmentation entails splitting a network into small but manageable segments. Network segmentation enhances both the security and performance of the network. In the event that a hacker accesses a part of a network, a segmented network can prevent the adversary from accessing other systems that are not connected to the same network. This is as opposed to an unsegmented network, where an adversary can move laterally, gaining access to all connected systems. Computers should be equipped with an automatic lock screen functionality. They should be set to lock automatically, say after three minutes of inactivity. This is to prevent unauthorized users from accessing the computer and the network in extension. In accordance with Section 10.4 of the Security Policy for the Government of Canada, contracting authorities must: Ensure security screening of private sector organizations and individuals who have access to protected and classified information and assets, as specified in the standards. Ensure safeguarding of government assets, including IT systems. Specify the necessary security requirements in terms and conditions in any contractual documentation.