CYBERSECURITY READINESS:
Discussion Guide

Michelle Neisen
President
ACP Capital of Texas Chapter
MODERATOR

Zoe Eslinger
Regional Sales Director-TOLA
LightBeam

Bill Alderson
Board Member
ISSA Austin

Table of Contents

Introduction

In this computerized era, cyber-security preparedness is the most crucial for the organizations of all types and sectors. With the ever-changing threat environment and the increasing complexity of attacks, it is necessary for businesses to be ahead of the curve in the protection of their assets, data, and reputation.

This book is a full guide to cybersecurity professionals, giving the views on the essential strategies, best practices, and the actionable steps to increase the cybersecurity preparedness. This manual will be the source of the vital details that will help you to cope with the complicated world of cybersecurity whether you are getting ready for a possible breach, analyzing the security posture of your organization, or dealing with the stakeholders.

The main steps that should be taken when you are confronted with a hack to the Board, can in a way, be put into three steps. Each chapter subsequently highlights the crucial topics for the Board to know to ensure that the organization is well-equipped to deal with cyber risks.

We have taken the input of the industry expert and the best practices thus offering us with the practical advice and the recommendations that can be applied to your organization's specific needs and challenges. No matter what your job is, whether it is an IT person, a cybersecurity manager, or a business leader, this book gives you the information and tools that you will need to improve your organization's cyber defenses.

The surge of cyber threats makes it need to be at the front of the curve. By adopting the strategies that are suggested in this guide and the building of a culture of cybersecurity awareness, you can cut the risks, safeguard your assets and thus, the future of your organization.

We will go through this journey together and thereby increase cybersecurity readiness and thus make a safer digital environment for everyone.

Preparing for a Hack: *Top Three Steps*

Containment:

The first step to be taken after the discovery of a cybersecurity breach is to contain it immediately to avoid the further damage to your systems, data, and reputation. Containment is the process of isolating the attacked systems and stopping the attacker from moving laterally within your network. Here's an in-depth look at each aspect: Here's an in-depth look at each aspect:

a. **Isolating Affected Systems:**
   - The systems and networks that were hit by the breach are being found. The solution may be the use of network monitoring tools, intrusion detection systems, and security incident and event management (SIEM) systems.
   - Fence off the systems that are already infected from the rest of the network to stop the attacker from going even further. This can be accomplished by cutting off the affected devices from the network, stopping suspicious network traffic, or setting up VLANs to isolate the compromised areas.
   - Create rules or access controls that will limit communication between the systems with compromised security and the rest of the network.

b. **Mitigating Data Loss:**
   - Determine and rank the essential data and assets that are vulnerable to loss and theft. Thus, the circumstances that are considered in this regard may include customer data, intellectual property, financial records, or sensitive corporate information.
   - Data loss prevention (DLP) measures should be used to stop unauthorized access or the exfiltration of sensitive data. Such field may be the encryption of data, the limitation of the access permissions, or the monitoring of the data flows for suspicious activities.
   - Keep the outgoing network traffic under check and see if there are any traces of data exfiltration, for instance, large file transfers or unusual network connections.

a. **Minimizing Impact and Scope: -**
   - Analyze the damage and the impact to the scope of the breach to know the level of the damage. This may be the case of performing a risk assessment to find out the systems, data, and the processes that are affected.
   - Direct the efforts of containment to the systems and data that are critical. Concentrate on the areas of high impact first to lessen the disturbance to businesses.
   - Convey the situation to the essential people, for instance, the senior management, IT teams, and legal counsel, to make sure that everyone is aware of the matter and that they know their functions in the containment process.

Forensics & Investigation:

Following the end of the breach, it is of utmost importance to carry out a complete investigation to figure out how the attack happened, which systems were involved, and the data that might have been stolen. The forensic analysis is the key factor in determining the reason of the breach and the evaluation of the scale of data invasion. Here's a detailed breakdown:

a. **Identifying Attack Vectors:**
   - The review of the logs, traffic, and other forensic evidence will help you to detect the initial attack vector used by the attacker. Among the types of cyber-attacks may include phishing emails, malware infections, unauthorized access, or software vulnerabilities.
   - Study malware samples or suspicious files that are proving to be controversial to find out about their behavior and functionality. Thus, it can reveal the kind of malware that was employed and its abilities.
   - Question the users who were affected or the IT staff to find out what they saw or noticed in the way of unusual activities or the activities that occurred before and during the breach.

b. **Assessing Scope and Impact:**
   - The first step is to do a complete showdown of the systems that are affected, including the servers, workstations, and network devices. Jot down any changes or the bizarre things you notice on these systems.
   - Use of network forensics tools to rebuild the attack timeline and to figure out the sequence of events that occurred before the breach is the best way to know the attacker. This might be a way of looking at the network traffic logs, firewall logs, and the intrusion detection system alerts.
   - Examine the effect of the breach on business activities, data protection and regulatory norms. Figure out what data was possibly breached, modified, or transmitted by the hacker.

c. **Collecting Evidence:**
   - The forensic evidence should be preserved and collected in accordance with the given guidelines to make it valid and incriminatory in court. This could be about the creation of forensic disk images, the capture of volatile memory, and the logging of the system artifacts.
   - The provenance chain of evidence is to be documented for the sake of its security and traceability. The process covers the registering of the persons who took the evidence, the time and place of its collection, and the information about its modification or damage.
   - Cooperate with legal counsel to make sure that forensic procedures follow legal and regulatory rules like chain of custody, data privacy laws, and evidence handling procedures.

d. **Reporting and Documentation:**
   - Write a complete report which will contain all the findings of the investigation, namely, the attack timeline, the attack vectors, the compromised systems, and the data that has been accessed or exfiltrated.
   - Come up with the solutions for the fix and the way to deal with the problem once the investigation is over. Such measures may be the combination of fixing the security bugs, strengthening the security mechanisms, and making the incident response system better.

- Besides, the investigation report must be forward to important people such as the senior management, IT teams, legal counsel, and regulatory authorities as the law demands.

Recovery & Remediation:

Once the breach is contained and investigated, the focus shifts to recovery and remediation efforts to restore affected systems, data, and services. Here's an in-depth look at each aspect:

a. **Restoring Systems from Backups:**
   - Identify and prioritize critical systems and data for restoration based on business needs and impact assessment.
   - Verify the integrity of backup data and ensure it has not been compromised or encrypted by the attacker. This may involve using offline or immutable backups stored in a secure location.
   - Restore affected systems from backups using established procedures and protocols. Ensure that restored systems are fully patched and updated to prevent re-infection.

b. **Implementing Remediation Measures:**
   - Patch vulnerabilities identified during the investigation to prevent future attacks. This may involve deploying software updates, firmware updates, or security patches provided by vendors.
   - Harden security controls and configurations to mitigate common attack vectors and reduce the risk of future breaches. This includes implementing least privilege access, disabling unnecessary services, and configuring firewalls and intrusion detection systems.
   - Conduct post-incident testing and validation to ensure that remediation measures are effective and do not introduce new vulnerabilities or issues.

c. **Communicating with Stakeholders:**
   - Keep key stakeholders informed of the recovery and remediation efforts, including senior management, IT teams, legal counsel, and regulatory authorities.
   - Provide regular updates on the progress of recovery efforts, including any challenges or obstacles encountered during the process.
   - Coordinate with external parties, such as vendors, customers, and business partners, to ensure they are aware of the situation and any potential impact on their operations.

d. **Lessons Learned and Continuous Improvement:**
   - Conduct a post-incident review to identify lessons learned and areas for improvement in the organization's cybersecurity posture and incident response capabilities.
   - Document the findings of the post-incident review and develop an action plan to address identified gaps and weaknesses.
   - Implement corrective actions and process improvements to enhance the organization's resilience to future cyber threats. This may include updating policies and procedures, enhancing staff training, and investing in new technologies or security controls.

Departments to Engage/Notify First:

Effective communication and collaboration with key departments are essential during a cybersecurity incident. Here's a detailed overview of who to engage and notify first:

a. **Incident Response Team:**
   - The incident response team is responsible for coordinating the organization's response to the breach, including containment, investigation, and recovery efforts.
   - Key members of the incident response team include the incident commander, forensic analysts, IT technicians, and legal counsel.
   - The incident response team should be activated immediately upon detection of a breach and should follow established incident response procedures and protocols.

b. **IT & Security Teams:**
   - The IT and security teams are responsible for managing and securing the organization's IT infrastructure and systems.
   - Notify the IT and security teams to assist with containment efforts, identify affected systems, and implement remediation measures.
   - IT technicians and security analysts should work closely with the incident response team to provide technical expertise and support during the incident.

c. **Legal & Compliance:**
   - Legal and compliance departments play a crucial role in ensuring that the organization's response to the breach complies with legal and regulatory requirements.
   - Legal counsel should be notified to provide guidance on breach notification laws, regulatory reporting requirements, and potential legal liabilities.
   - Compliance officers should assist with documenting the breach, assessing regulatory implications, and coordinating with regulatory authorities as required.

d. **PR/Communications:**
   - The PR and communications team is responsible for managing external communications and public relations during a cybersecurity incident.
   - Notify the PR and communications team to prepare for potential media inquiries, press releases, and customer notifications.
   - The PR team should work closely with the incident response team to ensure that all external communications are accurate, timely, and consistent.

Increasing Security Posture and Cyber Readiness

Risk Assessment:

Regularly conducting comprehensive risk assessments is essential for identifying and prioritizing security weaknesses within an organization's infrastructure. Here's an in-depth look at each step involved:

a. **Vulnerability Assessments:**
   - Utilize automated scanning tools and manual testing techniques to identify vulnerabilities in network devices, servers, applications, and other IT assets.
   - Prioritize vulnerabilities based on their severity, exploitability, and potential impact on business operations.
   - Assess the likelihood of exploitation for each vulnerability, considering factors such as the existence of known exploits, accessibility from the internet, and the presence of compensating controls.

b. **Penetration Testing:**
   - Conduct controlled attacks on the organization's systems and networks to identify potential security weaknesses and validate the effectiveness of existing controls.
   - Perform both internal and external penetration tests to simulate attacks from both inside and outside the organization's network perimeter.
   - Utilize ethical hacking techniques to exploit vulnerabilities and gain unauthorized access to sensitive systems and data.

c. **Threat Modeling:**
   - Analyze potential threats and attack vectors targeting the organization's assets, including data breaches, insider threats, malware infections, and denial-of-service attacks.
   - Create threat models to identify and prioritize the most critical threats based on their likelihood and potential impact.
   - Develop mitigation strategies and controls to address identified threats and vulnerabilities, considering factors such as cost-effectiveness and feasibility.

d. **Risk Prioritization and Mitigation:**
   - Use risk scoring frameworks such as the Common Vulnerability Scoring System (CVSS) or the FAIR (Factor Analysis of Information Risk) model to prioritize security weaknesses based on their impact and likelihood.
   - Implement mitigation measures to address identified risks, such as applying software patches, updating security configurations, and implementing additional security controls.
   - Regularly review and update the organization's risk register to reflect changes in the threat landscape and the effectiveness of mitigation efforts.

Continuous Training:

Ensuring that all staff members receive ongoing cybersecurity training is critical for building a culture of security awareness within the organization. Here's a detailed breakdown of effective training strategies:

a. **Awareness Programs:**
   - Develop and deliver cybersecurity awareness programs tailored to the organization's specific needs and risk profile.
   - Cover a wide range of topics, including phishing awareness, password hygiene, social engineering, data handling best practices, and incident reporting procedures.
   - Use a variety of training formats, such as e-learning modules, interactive workshops, and newsletters, to engage different learning styles.

b. **Phishing Simulations:**
   - Conduct regular phishing simulations to test employees' ability to recognize and report phishing emails.
   - Create realistic phishing scenarios that mimic common attack techniques, such as spoofed emails from trusted senders or urgent requests for sensitive information.
   - Provide immediate feedback and targeted training to employees who fall victim to phishing attacks, emphasizing the importance of vigilance and skepticism.

c. **Role-Based Training:**
   - Tailor training programs to the specific roles and responsibilities of different staff members within the organization.
   - Provide specialized training for IT and security teams, executives, HR staff, finance personnel, and other departments based on their unique security requirements.
   - Incorporate hands-on exercises and real-world scenarios to reinforce key concepts and skills relevant to each role.

d. **Continuous Learning and Certification:**
   - Encourage employees to pursue continuous learning and professional development in cybersecurity through industry certifications, workshops, and conferences.
   - Provide support for employees seeking certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or Certified Information Security Manager (CISM).
   - Recognize and reward employees who demonstrate a commitment to enhancing their cybersecurity skills and knowledge.

Zero-Day Drills:

Conducting regular drills to simulate zero-day attacks and other breach scenarios is essential for testing and improving the organization's incident response capabilities. Here's a detailed look at the key components of zero-day drills:

a. **Scenario Development:**
   - Develop realistic scenarios based on emerging threats, known vulnerabilities, and industry trends.
   - Include a variety of attack vectors and techniques, such as zero-day exploits, ransomware attacks, insider threats, and supply chain compromises.
   - Tailor scenarios to the organization's specific environment, business processes, and risk profile.

b. **Incident Response Simulation:**
   - Simulate the detection and initial response to a zero-day attack, including alert triage, incident validation, and escalation procedures.
   - Activate the organization's incident response team and follow established incident response playbooks and procedures.
   - Coordinate with external stakeholders, such as law enforcement agencies, incident response vendors, and regulatory authorities, as necessary.

Approaching the Board

When discussing cybersecurity readiness with the Board, it's essential to effectively communicate the importance of cybersecurity in terms of risk management and business continuity. Here's how to approach the Board:

Budget Allocation:

When presenting cybersecurity budget requirements to the Board, it's crucial to provide a clear breakdown of the investments needed to strengthen the organization's security posture. Here's a detailed approach:

a. **Comprehensive Budget Proposal:**
   - Prepare a detailed budget proposal outlining the specific cybersecurity initiatives and investments required to address existing vulnerabilities and mitigate potential risks.
   - Include budget estimates for technology upgrades, security tools and software, cybersecurity training programs, incident response capabilities, and third-party services such as penetration testing and security audits.

b. **Cost-Benefit Analysis:**
   - Conduct a cost-benefit analysis to demonstrate the potential financial impact of cyber threats on the organization.
   - Quantify the potential costs associated with data breaches, downtime, regulatory fines, legal fees, and reputational damage.
   - Highlight the cost-effectiveness of preventive measures compared to the potential costs of a security breach.

c. **c. Return on Investment (ROI):**
   - Articulate the expected ROI of cybersecurity investments in terms of risk reduction, improved operational efficiency, and enhanced business resilience.
   - Identify key performance indicators (KPIs) to measure the effectiveness of cybersecurity initiatives, such as reduced mean time to detect (MTTD) and mean time to respond (MTTR) to security incidents.

d. **d. Long-Term Strategic Planning:**
   - Align cybersecurity budget requirements with the organization's long-term strategic objectives and risk appetite.
   - Prioritize investments based on the organization's most critical assets, regulatory requirements, and industry best practices.
   - Advocate for a multi-year budget plan to ensure sustained funding for cybersecurity initiatives and ongoing improvements.

Management Oversight:

Emphasizing the need for Board oversight in cybersecurity matters is essential for ensuring that cybersecurity is treated as a strategic priority. Here's a detailed approach:

a. **Regular Updates and Reporting:**
   - Provide regular updates to the Board on cybersecurity initiatives, emerging threats, and incident response capabilities.
   - Present quarterly or annual reports on cybersecurity performance, highlighting key metrics, trends, and areas for improvement.
   - Ensure that cybersecurity updates are included on the agenda of Board meetings and executive briefings.

b. **Risk Assessments and Compliance:**
   - Conduct regular risk assessments to identify and prioritize cybersecurity risks facing the organization.
   - Present risk assessment findings to the Board, emphasizing the potential impact of identified risks on business operations and objectives.
   - Provide updates on regulatory compliance requirements and the organization's efforts to maintain compliance with relevant laws and standards.

c. **Incident Response Planning:**
   - Review and approve incident response plans and procedures developed by the cybersecurity team.
   - Conduct tabletop exercises and simulations to test the organization's incident response capabilities and coordination with external stakeholders.
   - Ensure that the Board is briefed on the organization's readiness to respond to various types of cyber incidents, including data breaches, ransomware attacks, and supply chain compromises.

d. **Strategic Direction Setting:**
   - Engage the Board in discussions about the organization's cybersecurity strategy and long-term goals.
   - Seek input from Board members on key cybersecurity decisions, such as technology investments, risk management strategies, and policy development.
   - Encourage the Board to adopt a proactive approach to cybersecurity governance, emphasizing the importance of staying ahead of evolving threats.

Personnel and Skillset:

Highlighting the importance of skilled cybersecurity personnel and continuous training is critical for ensuring that the organization is well-equipped to address cyber threats effectively. Here's a detailed approach:

a. **Talent Recruitment and Retention:**
   - Provide an overview of the organization's current cybersecurity team, including roles, responsibilities, and skillsets.
   - Highlight the challenges and competition in recruiting and retaining cybersecurity talent in a competitive market.
   - Present strategies for attracting and retaining top cybersecurity professionals, such as competitive compensation packages, professional development opportunities, and a positive work culture.

b. **Continuous Training and Development:**
   - Showcase the organization's commitment to ongoing cybersecurity training and development for all staff members.
   - Highlight the various training programs and resources available to enhance employees' cybersecurity knowledge and skills.
   - Provide examples of successful training initiatives, such as phishing simulations, cybersecurity awareness campaigns, and role-based training programs.

c. **Collaboration with Academic Institutions:**
   - Explore partnerships with academic institutions to develop cybersecurity talent pipelines and internship programs.
   - Highlight initiatives to sponsor cybersecurity research, collaborate on curriculum development, and engage with student cybersecurity organizations.
   - Discuss the benefits of recruiting interns and graduates with specialized cybersecurity degrees or certifications.

d. **Leadership Support and Advocacy:**
   - Secure buy-in and support from executive leadership for investing in cybersecurity talent and training.
   - Demonstrate the link between skilled cybersecurity personnel and the organization's ability to detect, respond to, and recover from cyber threats.

Defining Cybersecurity Maturity Stages

Cybersecurity maturity can be categorized into several stages, each reflecting the organization's level of preparedness and capability to manage cyber risks. Here's a general breakdown:

Stage 1 - Ad Hoc:

At this stage, cybersecurity efforts are reactive and ad hoc, with no formal processes or controls in place. The organization lacks awareness of its cybersecurity risks and may have limited resources dedicated to cybersecurity.

Stage 2 - Defined:

The organization begins to establish formal cybersecurity policies, procedures, and controls. There's a growing awareness of cyber risks, and basic security measures are implemented. However, these measures may not be consistently applied across the organization.

Stage 3 - Managed:

In this stage, the organization implements a proactive approach to cybersecurity. There's active monitoring of security controls, regular risk assessments, and incident response plans in place. Security measures are continuously updated based on emerging threats and vulnerabilities.

Stage 4 - Measured:

At this stage, the organization focuses on measuring and improving its cybersecurity effectiveness. Key performance indicators (KPIs) and metrics are used to assess the efficiency of security controls and incident response capabilities. Continuous improvement is a key focus.

Stage 5 - Optimized:

In the final stage, cybersecurity is fully integrated into the organization's culture and business processes. The organization has matured its cybersecurity capabilities to a level where it can effectively identify, respond to, and recover from cyber threats. There's a strong emphasis on innovation and adapting to emerging threats.

Mitigating Risk with Third Parties

Risk Assessment:

Conducting thorough risk assessments of third-party vendors is essential for identifying and prioritizing potential security risks associated with outsourcing. Here's an in-depth look at each step involved:

a. **Vendor Selection Criteria:**
   - Define criteria for selecting third-party vendors, including factors such as reputation, financial stability, geographic location, and industry expertise.
   - Prioritize vendors with a strong commitment to cybersecurity and a demonstrated track record of compliance with security standards.

b. **Security Posture Evaluation:**
   - Assess the security posture of third-party vendors by evaluating their security policies, procedures, and controls.
   - Review documentation such as security policies, incident response plans, and security assessment reports to assess the maturity of the vendor's security program.
   - Conduct on-site visits or virtual assessments to verify the effectiveness of the vendor's security controls.

c. **Data Handling Practices:**
   - Evaluate how third-party vendors handle and protect sensitive data, including customer information, intellectual property, and proprietary business data.
   - Assess data encryption practices, access controls, data retention policies, and data disposal procedures to ensure compliance with data protection regulations.
   - Identify any potential risks associated with the transmission, storage, or processing of sensitive data by third-party vendors.

d. **Compliance with Security Standards:**
   - Verify that third-party vendors comply with relevant security standards and regulations, such as ISO 27001, SOC 2, GDPR, HIPAA, or PCI DSS.
   - Request copies of compliance certificates, audit reports, and attestation letters to validate the vendor's adherence to security requirements.
   - Ensure that third-party vendors undergo regular security assessments and audits to maintain compliance.

e. **Risk Prioritization and Mitigation:**
   - Prioritize identified risks based on their potential impact on the organization and the likelihood of occurrence.
   - Develop mitigation strategies and controls to address high-risk areas, such as implementing additional security controls, requiring regular security updates, or limiting access to sensitive data.

- Document risk assessment findings and mitigation strategies in a formal risk register or risk management framework.

Contractual Agreements:

Including robust security clauses in contracts with third-party vendors is crucial for defining security responsibilities and mitigating risks. Here's an in-depth look at the key components of contractual agreements:

a. **Security Responsibilities:**
   - Clearly define the security responsibilities of both the organization and the third-party vendor in the contract.
   - Specify the security controls and measures that the vendor must implement to protect the organization's data and assets.
   - Outline the roles and responsibilities of each party in detecting, reporting, and responding to security incidents.

b. **Data Protection Measures:**
   - Include clauses specifying the data protection measures that the vendor must implement to safeguard sensitive data.
   - Require the vendor to encrypt data both in transit and at rest, implement access controls, and regularly monitor and audit access to sensitive data.
   - Define data handling and processing requirements to ensure compliance with data protection regulations.

c. **Breach Notification Procedures:**
   - Establish clear procedures for reporting security incidents and data breaches to the organization.
   - Define the timeline and method for notifying the organization of any security incidents or data breaches.
   - Require the vendor to provide detailed incident reports, including the root cause of the incident, the impact on the organization, and the remediation steps taken.

d. **Liability in Case of Security Incident:**
   - Define the liability of the vendor in case of a security incident or data breach.
   - Specify the financial penalties, indemnification clauses, and liability limitations applicable to the vendor in the event of a security incident.
   - Ensure that the contract includes provisions for compensating the organization for any damages resulting from the vendor's failure to comply with security requirements.

e. **Compliance with Standards and Regulations:**
   - Require the vendor to comply with industry standards, regulatory requirements, and best practices related to cybersecurity.
   - Include clauses requiring the vendor to undergo regular security assessments, audits, and compliance checks.

- Ensure that the contract allows the organization to terminate the agreement in case of non-compliance with security requirements.

Ongoing Monitoring:

Continuously monitoring third-party vendors is essential for ensuring ongoing compliance with security requirements and identifying any emerging risks or issues. Here's a detailed approach to ongoing monitoring:

a. **Regular Audits and Assessments:**
   - Conduct regular audits and security assessments of third-party vendors to verify compliance with security requirements.
   - Schedule on-site visits, virtual assessments, or remote audits to evaluate the effectiveness of the vendor's security controls.
   - Use standardized assessment frameworks or questionnaires to streamline the auditing process and ensure consistency.

b. **Security Performance Reviews:**
   - Review the vendor's security performance on a regular basis to identify any trends or patterns indicating potential security issues.
   - Monitor key security metrics, such as patch management compliance, incident response times, and security incident trends.
   - Compare the vendor's security performance against industry benchmarks and best practices.

c. **Incident Response Monitoring:**
   - Monitor the vendor's incident response capabilities and procedures to ensure timely detection and response to security incidents.
   - Require the vendor to provide incident reports and post-incident analyses for any security incidents that occur.
   - Conduct joint tabletop exercises and incident response drills with the vendor to test their incident response readiness.

d. **Contractual Compliance Checks:**
   - Review the vendor's compliance with contractual security requirements on a regular basis.
   - Ensure that the vendor is implementing the security controls and measures outlined in the contract.
   - Address any discrepancies or non-compliance issues through corrective action plans and follow-up audits.

Ensuring Non-IT Members' Cybersecurity Readiness

Cybersecurity readiness extends beyond the IT department to involve all members of an organization. Here's how to ensure non-IT members are prepared:

1. **Training and Awareness:**
    a. Provide regular cybersecurity training and awareness programs for all staff members, including executives, regular employees, temp workers, contractors, and suppliers. Cover topics such as phishing awareness, password hygiene, data handling best practices, and incident reporting procedures.
2. **Role-Based Training:**
    b. Tailor training programs based on the specific roles and responsibilities of non-IT staff members. For example, executives may need training on cybersecurity governance and risk management, while regular employees may need training on secure data handling practices.
3. **Supplier and Contractor Requirements:**
    c. Include cybersecurity requirements in contracts with suppliers and contractors, outlining their responsibilities for protecting sensitive information and complying with security standards. Ensure that third-party suppliers are vetted for their cybersecurity practices.
4. **Executive Leadership Support:**
    d. Gain support from executive leadership to prioritize cybersecurity readiness across the organization. Ensure that cybersecurity initiatives are aligned with business objectives and that resources are allocated appropriately.