INFORMATION ASSURANCE PLAN

Organization: T-Mobile

MARCH 9, 2025

Juliano Alves de Souza

I. Information Assurance Plan Introduction

a. Overview of Goals and Objectives

The goal of this Information Assurance (IA) Plan is to develop a comprehensive strategy to protect T-Mobile's sensitive data and ensure the **confidentiality, integrity, and availability (CIA)** of information assets. These three principles form the foundation of information security and are essential for maintaining customer trust, complying with regulatory standards, and protecting the organization's operational continuity. The IA plan aims to mitigate vulnerabilities, strengthen existing security protocols, and ensure continuous monitoring and incident response capabilities.

Creating and maintaining an IA plan centered around CIA principles provides several key benefits. It reduces the likelihood of unauthorized data access (**confidentiality**), ensures that data is accurate and unaltered during its lifecycle (**integrity**), and guarantees that data and systems remain accessible to authorized users when needed (**availability**) (CISA, 2023). For T-Mobile, this is critical given the 2021 data breach that exposed sensitive information for over 76 million customers, highlighting the need for improved safeguards to protect personally identifiable information (PII), customer trust, and business reputation (Verizon, 2023).

b. Confidentiality, Integrity, and Availability of Information

An accurate assessment of T-Mobile's confidentiality, integrity, and availability of information reveals significant vulnerabilities exposed by the 2021 data breach.

1. **Confidentiality:**

   Confidentiality is one of the primary areas of concern, as the breach revealed sensitive

data, including Social Security numbers, driver's license information, and account PINs. This indicates insufficient encryption, poor access control, and misconfigured servers that allowed unauthorized access to customer data (Progress Software, 2023).

2. **Integrity:**

   Data integrity was also at risk due to the lack of sufficient safeguards to detect or prevent unauthorized modifications to sensitive information. The absence of robust monitoring systems left T-Mobile unable to identify and respond to anomalies in real-time, creating potential opportunities for tampering with data during the attack (CISA, 2023).

3. **Availability:**

   While no major outages were reported during the breach, the incident underscores a potential lack of resilient disaster recovery mechanisms. Downtime or denial-of-service (DoS) events could have been devastating, given the organization's reliance on continuous data availability to provide seamless telecommunication services to its customers (Verizon, 2023).

c. Current Protocols and Policies

T-Mobile has implemented some security protocols and policies to safeguard customer data, but deficiencies in their application and enforcement have left critical gaps. Current measures include:

- **Encryption Standards:** T-Mobile encrypts some sensitive data, but the breach suggests insufficient application of encryption to all at-risk data (CISA, 2023).

- **Access Controls:** While access controls exist, misconfigured servers during the 2021 breach indicate that these controls were either poorly managed or not consistently applied (Progress Software, 2023).
- **Incident Response:** T-Mobile has an incident response plan, as evidenced by their notification and remediation efforts post-breach, but the lack of proactive detection mechanisms allowed attackers to access the systems undetected for an extended period (Verizon, 2023).

- **Deficiencies:**
  Key deficiencies include:

  1. **Data Retention Policies:** T-Mobile stored sensitive data from prospective and former customers for longer than necessary, increasing its risk exposure (Verizon, 2023).
  2. **Vulnerability Management:** Misconfigured servers and delayed detection suggest inadequate patch management, system monitoring, and threat assessment processes (Progress Software, 2023).
  3. **Third-Party Vendor Oversight:** As a large telecom provider, T-Mobile relies heavily on third-party software and vendors. A lack of stringent third-party risk assessments and contractual security requirements contributed to the breach (CISA, 2023).

- **Potential Barriers to Implementation**
  Implementing a robust information assurance plan may encounter the following barriers:

  1. **Organizational Resistance:** Changes to existing policies, particularly those that require extensive reconfiguration of legacy systems, may face resistance from internal teams and stakeholders (Verizon, 2023).

  2. **Budget Constraints:** Significant investment in security technologies, third-party audits, and staff training may strain financial resources (CISA, 2023).

  3. **Complexity of Existing Infrastructure:** T-Mobile's large and complex infrastructure, which includes legacy systems, cloud services, and third-party tools, could create challenges in aligning all components with the IA plan (Progress Software, 2023).

  4. **Regulatory and Compliance Pressure:** Compliance with diverse regulatory requirements, including **GDPR**, **CCPA**, and telecom-specific laws, can increase the complexity of implementing and maintaining the IA plan (Verizon, 2023).

II. Information Security Roles and Responsibilities

a. Key Leaders and Their Responsibilities in Information Security

In any organization, the security of information is a shared responsibility among key leaders who oversee various aspects of information assurance. Their roles are interconnected, ensuring a

comprehensive security strategy that protects sensitive data, maintains regulatory compliance, and fosters a culture of security awareness.

1. **Chief Executive Officer (CEO)** – The CEO provides overall strategic direction and is responsible for setting the tone for cybersecurity policies. While they may not be directly involved in day-to-day security operations, they play a crucial role in ensuring that information security is a priority and that adequate resources are allocated to cybersecurity initiatives. According to Smith et al. (2021), CISOs must align security strategies with business objectives while managing cyber threats effectively.
2. **Chief Information Security Officer (CISO)** – The CISO is the primary executive responsible for developing, implementing, and managing the organization's information security program. This includes risk assessments, security policies, incident response planning, and compliance with legal and regulatory standards. The CISO collaborates closely with other leaders to ensure security aligns with business objectives.
3. **Chief Information Officer (CIO)** – The CIO oversees IT infrastructure and ensures that security measures are integrated into technology solutions. The CIO works alongside the CISO to balance security with operational efficiency, ensuring the availability of critical business systems while minimizing security risks.
4. **Chief Compliance Officer (CCO)** – The CCO ensures that the organization adheres to legal and regulatory requirements related to cybersecurity and data protection. They monitor compliance with laws such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and the National Institute of Standards and Technology (NIST) framework, depending on the industry.

5. **Security Analysts and IT Staff** – Security analysts and IT professionals are responsible for monitoring security systems, identifying vulnerabilities, and responding to incidents. They play a hands-on role in implementing security controls, managing access, and maintaining the integrity of systems.

These roles are interconnected, as a failure in one area can have a cascading impact on the entire security posture. The CEO must support the CISO's initiatives, the CIO must align IT strategies with security policies, and the CCO must ensure compliance across the board.

b. Ethical and Legal Considerations in Information Assurance

Key leaders in an organization must address ethical and legal considerations in their information assurance strategies. Ethical considerations include respecting user privacy, ensuring transparency in data collection, and protecting sensitive information from unauthorized access. Legal considerations include compliance with data protection laws, industry regulations, and corporate governance requirements.

Failure to properly address these considerations can have severe ramifications, such as:

- **Legal Penalties** – Non-compliance with regulations like **GDPR, HIPAA, or the Sarbanes-Oxley Act (SOX)** can result in significant fines and legal action.
- **Reputational Damage** – A security breach caused by negligence or unethical behavior can erode customer trust and impact brand reputation.

- **Financial Losses** – Cybersecurity incidents can lead to costly litigation, regulatory fines, and loss of business revenue due to downtime or data theft.
- **Operational Disruptions** – Poorly managed security policies can lead to data breaches, ransomware attacks, and system outages that disrupt business operations.

By establishing clear ethical and legal guidelines within the information assurance plan, leaders can mitigate risks and ensure that security practices align with regulatory and industry standards.

c. Key Components of Information Assurance in Roles and Responsibilities

Information assurance is built upon three core principles: **Confidentiality, Integrity, and Availability (CIA Triad)**. These principles must be reflected in the roles and responsibilities of organizational leaders and employees.

1. **Confidentiality** – Ensuring that sensitive data is only accessible to authorized users.
    - **CISO & Security Analysts**: Implement access controls, encryption, and authentication mechanisms.
    - **CIO**: Ensures secure data storage and transmission practices.
    - **Employees**: Follow best practices for password management and avoid unauthorized data sharing.
2. **Integrity** – Maintaining the accuracy and reliability of data.

- **CISO & Security Analysts**: Deploy monitoring tools and implement data integrity verification measures.
- **CIO**: Ensures proper system updates and patch management.
- **Employees**: Avoid actions that compromise data integrity, such as unauthorized modifications.

3. **Availability** – Ensuring that information and systems remain accessible when needed.
   - **CIO**: Implements redundancy measures, disaster recovery, and system backups.
   - **CISO & IT Staff**: Monitor systems for potential cyber threats and mitigate downtime risks.
   - **Employees**: Follow IT security protocols to prevent inadvertent disruptions.

By assigning clear roles and responsibilities within the information assurance plan, organizations can build a resilient cybersecurity framework that protects data assets, supports regulatory compliance, and maintains trust with stakeholders.

III. Risk Assessment

a. Analyze the Environment in Which the Organization Operates

T-Mobile operates in the highly regulated telecommunications sector, managing vast volumes of sensitive customer data, including personally identifiable information (PII), payment details, and communication records. The organization's IT environment comprises cloud services, legacy systems, and third-party vendor integrations, creating a complex attack surface.

Current Protocols and Policies Related to Information Assurance:

- **Encryption Standards:** Partial encryption of sensitive data in transit and at rest, though the 2021 breach revealed gaps in encrypting all at-risk data (CISA, 2023).
- **Access Controls:** Role-based access control (RBAC) is implemented, but misconfigured servers during the breach exposed weaknesses in policy enforcement (Progress Software, 2023).
- **Incident Response Plan:** Post-breach remediation efforts exist, but delayed detection of the 2021 attack highlighted deficiencies in proactive monitoring (Verizon, 2023).
- **Third-Party Risk Management:** Limited oversight of vendor security practices contributed to the breach (CISA, 2023).

Key Challenges:

1. Legacy systems complicating patch management.
2. Over-retention of customer data, increasing exposure risks (Verizon, 2023).
3. Insufficient employee training in phishing and social engineering.

b. Evaluate the Threat Environment of the Organization

T-Mobile faces a dynamic threat landscape, as evidenced by the 2021 breach that compromised data for 76 million customers. Key threats include:

External Threats

- **Phishing/Malware:** Attackers exploited unpatched vulnerabilities to deploy ransomware (Verizon, 2023).
- **Advanced Persistent Threats (APTs):** Sophisticated actors targeted misconfigured servers to exfiltrate data (Progress Software, 2023).
- **DDoS Attacks:** Potential to disrupt telecom services, impacting availability.

Internal Threats:

- **Insider Risks:** Employees with excessive privileges or poor security practices.
- **Accidental Data Exposure:** Weak access controls allowed unauthorized access during the breach (CISA, 2023).
- **Third-Party Risks:** Vendors with inadequate security practices introduced vulnerabilities into T-Mobile's network (Verizon, 2023).

c. Best Approaches for Implementing Information Assurance Principles

Recommended Approaches:

Layered Security (Defense in Depth):

Firewalls/IDS: Deploy next-gen firewalls and intrusion detection systems to monitor traffic, addressing misconfigured server vulnerabilities (Progress Software, 2023).

Zero Trust Architecture: Require continuous authentication for all users and devices, mitigating insider and third-party risks (NIST, 2020).

Enhanced Encryption and Access Controls:

Encrypt all sensitive data at rest and in transit using TLS 1.3 (OWASP, 2023).

Implement multi-factor authentication (MFA) and least privilege access to reduce unauthorized access (CISA, 2023).

Proactive Threat Intelligence:

Integrate threat intelligence feeds to identify emerging risks, such as APTs targeting telecom infrastructure (Verizon, 2023).

Employee Training:

Conduct mandatory phishing simulations and cybersecurity awareness programs to reduce human error.

Areas for Improvement in Current Protocols:

Patch Management: Automate updates to address unpatched software vulnerabilities (Progress Software, 2023).

Third-Party Audits: Enforce contractual security requirements for vendors and conduct biannual audits.

Data Retention Policies: Delete unnecessary customer data to minimize breach impacts (GDPR, 2016).

d. Risk Matrix

Threat	Vulnerability	Risk Level	Mitigation Strategy	Reference
Phishing Attacks	Lack of employee awareness	High	Mandatory security training and phishing simulations.	(OWASP, 2023)
Malware/Ransomware	Unpatched software	High	Automated patch management and endpoint protection tools (e.g., EDR).	(CISA, 2023)
Insider Threats	Weak access controls	Medium	Enforce MFA and implement user behavior analytics (UBA).	(NIST, 2020)
APTs	Misconfigured servers	High	Regular vulnerability scanning and server configuration audits.	(Verizon, 2023)
Third-Party Risks	Poor vendor security practices	Medium	Require vendors to comply with NIST 800-171 and conduct third-party risk assessments.	(CISA, 2023)
DDoS Attacks	Inadequate network defenses	Medium	Deploy cloud-based DDoS protection services (e.g., AWS Shield).	(OWASP, 2023)

IV. Statements of Policy

a. Incident Response Protocols

To effectively respond to cyber threats and vulnerabilities, the following Incident Response Protocol (IRP) will be implemented:

1. **Preparation:** Regular training, phishing simulations, and system hardening to prevent incidents.
2. **Detection and Analysis:** Deploy Security Information and Event Management (SIEM) tools to detect and analyze threats in real-time.
3. **Containment:** Isolate affected systems to prevent further spread of malware or data breaches.
4. **Eradication:** Conduct forensic analysis to remove threats and patch vulnerabilities.
5. **Recovery:** Restore systems using backups and validate system integrity before resumption.
6. **Post-Incident Review:** Conduct root cause analysis and update security policies accordingly.

b. Justification of Incident Response Protocols

Implementing a structured IRP minimizes downtime, reduces the impact of cyber threats, and ensures compliance with industry regulations such as NIST 800-61 (Incident Response Guide).

Given that T-Mobile faced a breach exposing 76 million customer records due to poor monitoring (Verizon, 2023), an improved IRP ensures proactive threat detection and rapid incident handling.

c. Disaster Response Protocols

A Disaster Recovery Plan (DRP) will be established to ensure business continuity in case of catastrophic cyber incidents, natural disasters, or system failures:

1. **Business Impact Analysis (BIA):** Identify critical systems and prioritize recovery efforts.
2. **Redundant Backups:** Implement offsite, cloud-based, and on-premise backups with encryption.
3. **Failover Systems:** Deploy redundant network paths and data centers to ensure service availability.
4. **Disaster Recovery Testing:** Conduct quarterly tabletop exercises and penetration tests to verify effectiveness.
5. **Communication Plan:** Define clear roles for IT teams, leadership, and external vendors during disaster recovery.

d. Justification of Disaster Response Protocols

A structured DRP ensures minimal service disruptions and prevents denial-of-service (DoS) attacks from crippling operations. Research highlights that organizations with robust disaster recovery plans recover 96% faster than those without (CISA, 2023). Given T-Mobile's reliance on real-time services, failover systems and redundant backups will mitigate downtime risks.

e. Access Control Protocols

To strengthen user authentication and system access while maintaining operational efficiency, the following Access Control Protocols will be implemented:

1. **Role-Based Access Control (RBAC):** Limit user access based on job roles to minimize insider threats.
2. **Multi-Factor Authentication (MFA):** Enforce MFA across all critical systems and remote access points.
3. **Zero Trust Architecture (ZTA):** Require continuous verification of users, devices, and network segments.
4. **Least Privilege Principle (PoLP):** Restrict admin privileges to reduce the risk of credential-based attacks.
5. **Biannual Access Reviews:** Conduct audits every six months to avoid unnecessary access.

f. Justification of Access Control Protocols

Access control policies prevent unauthorized data exposure, as seen in T-Mobile's breach, where misconfigured servers led to unauthorized access. According to NIST 800-53 (Security and Privacy Controls), implementing RBAC and MFA can reduce account compromises by 99.9% (CISA, 2023). The Zero Trust Model ensures no implicit trust is given to any user or device, reducing insider threats ahead.

g. Maintaining the Information Assurance Plan

To ensure continued effectiveness, the Information Assurance Plan (IAP) will be regularly updated using the following strategies:

Ongoing Employee Training and Security Awareness: Human error remains one of the leading causes of cybersecurity breaches. According to the 2023 IBM Cost of a Data Breach Report, organizations that implemented regular cybersecurity training for employees reduced the likelihood of social engineering attacks by 60% (IBM, 2023). Quarterly training sessions, phishing simulations, and security awareness programs reinforce best practices for password management, email security, and incident reporting, significantly reducing insider risks.

Continuous Security Monitoring: Regular monitoring and analysis of network traffic, system logs, and user activity help detect and prevent security incidents before they escalate. According to the National Institute of Standards and Technology (NIST) Special Publication 800-137, continuous monitoring enables organizations to identify vulnerabilities in real time, assess

security controls, and implement rapid corrective actions. Threat intelligence platforms, such as those provided by Cybersecurity and Infrastructure Security Agency (CISA), also help organizations stay ahead of emerging attack trends, ransomware threats, and zero-day vulnerabilities (CISA, 2023).Ongoing Employee Training: Conduct security awareness training every quarter.

Policy Revision and Compliance Audits: Cyber threats evolve rapidly, making it essential to periodically review and update security policies, procedures, and configurations. Industry's best practices, such as NIST 800-39 (Risk Management Framework), recommend biannual reviews of security policies to ensure alignment with current threat landscapes. Additionally, adopting an adaptive security architecture—which includes AI-driven threat detection and automated patch management—allows organizations to respond to new vulnerabilities without delays (Gartner, 2023).

Third-Party Risk Management: Many security breaches originate from third-party vendors with weak cybersecurity measures. A study by Ponemon Institute (2023) found that over 51% of organizations experienced a data breach caused by third-party vulnerabilities. Implementing vendor security assessments, contractual security requirements (such as NIST 800-171), and biannual audits ensure that external partners adhere to high security standards, preventing supply chain attacks.

h. Justification for Maintaining the Information Assurance Plan

Cyber threats evolve rapidly, making continuous monitoring and risk assessments critical. A 2023 study found that 74% of breaches involved human error (Verizon, 2023), underscoring the

need for regular training. Compliance audits ensure that the IAP remains aligned with regulatory requirements, reducing legal and financial liabilities.

V. Conclusion

T-Mobile's need for a robust Information Assurance (IA) Plan is underscored by the critical vulnerabilities exposed in the 2021 data breach, which compromised the personally identifiable information (PII) of over 76 million customers. This incident highlights the urgency of protecting sensitive data, restoring customer trust, and ensuring business continuity in a highly regulated telecommunications environment. An effective IA plan is essential to safeguard the confidentiality, integrity, and availability (CIA) of information assets, aligning with industry best practices and mitigating risks such as unauthorized access, data tampering, and service disruptions (Verizon, 2023; Easttom, 2023, Chapter 1).

Legally, T-Mobile is obligated to comply with regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the National Institute of Standards and Technology (NIST) frameworks, which mandate stringent data protection measures (European Union, 2016). Failure to implement and maintain an IA plan risks substantial fines, legal penalties, and operational disruptions. Ethically, T-Mobile has a responsibility to respect customer privacy, ensure transparency in data handling, and protect PII from misuse, as breaches erode trust and damage the organization's reputation (CISA, 2023). The 2021 breach, exacerbated by deficiencies in encryption, access controls, and third-party oversight, emphasizes the need for a proactive IA strategy to prevent future incidents, reduce financial liabilities, and uphold T-Mobile's position as a leading telecom provider.

A well-defined IA plan addresses these legal and ethical imperatives by establishing a framework to detect, respond to, and recover from cyber threats while fostering a security-conscious culture. Continuous monitoring, employee training, and policy updates are vital to adapt to evolving risks, ensuring compliance and operational resilience (NIST, 2011). Ultimately, this plan is not just a technical necessity but a strategic commitment to ethical stewardship and legal accountability.

The key elements of this IA plan—incident response protocols, disaster response protocols, access control protocols, and maintenance strategies—are designed to address T-Mobile's identified vulnerabilities and align with best practices from NIST, CISA, and industry research. Each element is assigned to specific organizational roles to ensure effective implementation, with clear incident response contacts established.

Incident Response Protocols

Description: These protocols include preparation (training and system hardening), detection/analysis (SIEM tools), containment, eradication, recovery, and post-incident review. They ensure rapid threat mitigation and minimize breach impact (NIST 800-61; Easttom, 2023, Chapter 7).

Responsible Party: The Chief Information Security Officer (CISO) oversees development and execution, supported by Security Analysts and IT Staff who implement monitoring and containment measures.

Defense: The 2021 breach's delayed detection underscores the need for proactive monitoring and structured response, reducing downtime and data exposure (Verizon, 2023).

Incident Contact: CISO (primary) and IT Team Lead.

Disaster Response Protocols

Description: A Disaster Recovery Plan (DRP) with business impact analysis, redundant backups, failover systems, testing, and a communication plan ensures business continuity during catastrophic events (CISA, 2023).

Responsible Party: The Chief Information Officer (CIO) manages IT infrastructure and backup systems, collaborating with the CISO for testing and recovery validation.

Defense: Research shows a 96% faster recovery with robust DRPs, critical for T-Mobile's real-time services (CISA, 2023; Easttom, 2023, Chapter 8).

Incident Contact: CIO (primary) and CISO.

Access Control Protocols

Description: Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Zero Trust Architecture (ZTA), least privilege principles, and biannual audits prevent unauthorized access while maintaining usability (NIST, 2020).

Responsible Party: The CISO implements access policies, with Security Analysts enforcing MFA and audits; the CIO ensures system integration.

Defense: These measures address the 2021 misconfigured server issue, reducing breaches by 99.9% (NIST 800-53; CISA, 2023; Easttom, 2023, Chapter 5).

Incident Contact: CISO (primary) and Security Analysts.

Maintenance Strategies

Description: Ongoing training, continuous monitoring, policy revisions, and third-party risk management keep the IA plan effective against evolving threats (NIST 800-137; Ponemon Institute, 2023).

Responsible Party: The CISO drives training and monitoring, the Chief Compliance Officer (CCO) oversees audits and compliance, and the CIO supports infrastructure updates.

Defense: With 74% of breaches tied to human error, regular training and monitoring are critical (Verizon, 2023; Easttom, 2023, Chapter 9).

Incident Contact: CISO (primary) and CCO: The Chief Executive Officer (CEO) provides overarching support, ensuring resources and strategic alignment, while all employees are responsible for adhering to security policies. In the event of an incident, the CISO serves as the primary contact, coordinating with the CIO, Security Analysts, and IT Team Lead based on the type of incident (e.g., breach vs. outage). This structure ensures accountability, rapid response, and long-term resilience, addressing T-Mobile's past deficiencies and safeguarding its future.

References

1. Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Confidentiality, integrity, and availability (CIA): Understanding key concepts*. U.S. Department of Homeland Security. https://www.cisa.gov/
2. European Union. (2016). *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu
3. National Institute of Standards and Technology (NIST). (2020). *Zero trust architecture*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
4. Open Web Application Security Project (OWASP). (2023). *Authentication cheat sheet*. https://owasp.org/
5. Progress Software. (2023). *Mitigating risks in file transfer software*. https://www.progress.com/
6. Verizon. (2023). *2023 Data breach investigations report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/
7. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). https://www.nist.gov
8. European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union. https://gdpr-info.eu
9. U.S. Department of Health & Human Services. (1996). Health Insurance Portability and Accountability Act (HIPAA). https://www.hhs.gov/hipaa
10. Gartner. (2023). *Adapting security strategies for evolving threats: The role of adaptive security architecture.* Gartner Research. https://www.gartner.com
11. IBM Security. (2023). *Cost of a data breach report 2023.* IBM Security. https://www.ibm.com/security/data-breach
12. National Institute of Standards and Technology (NIST). (2011). *Guide for continuous monitoring of information systems and organizations (SP 800-137).* U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-137.pdf
13. National Institute of Standards and Technology (NIST). (2010). *Managing information security risk: Organization, mission, and information system view (SP 800-39).* U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
14. Ponemon Institute. (2023). *The state of third-party risk management: How vendor vulnerabilities impact cybersecurity.* Ponemon Research. https://www.ponemon.org
15. Verizon. (2023). *2023 Data breach investigations report (DBIR).* Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/