CW1

CISO’s manual For incident Pre-active awareness

With the increasing frequency and severity of cyberattacks, it is essential to have a robust plan in place to protect your company's digital assets. This comprehensive checklist can assist you in evaluating your current security measures and identifying any vulnerabilities that may put your organization at risk.

In today's digital age, data security incidents are a constant threat to any organization that handles sensitive information. As such, it is crucial for every employee to be actively responsible in preventing such incidents from happening.

Being responsible means being aware of the potential risks and actively taking steps to mitigate them. It means staying informed about the latest security threats and vulnerabilities and being vigilant in identifying and reporting any suspicious activity.

One of the most important aspects of data security is employee training. Every employee should be trained on how to handle sensitive data, how to recognize potential security threats, and how to respond in the event of a security incident. This includes everything from basic security protocols, such as password management and encryption, to more advanced topics such as social engineering and phishing attacks.

As a CISO, your responsibility is not just to protect your organization's data, but also to ensure that your employees are trained to identify and respond to potential threats. With this checklist, you can be confident that you have taken all the necessary steps to safeguard your organization's assets and maintain the trust of your customers and stakeholders.

To help you prevent breaches and protect your organization's assets, we have created a comprehensive checklist of the key areas you need to be aware of. This checklist covers everything from employee training and access controls to incident response planning and disaster recovery.

Organisational

- [ ] Define the scope of the ISMS in accordance with the IEC/ISO27001 standards and policies to prevent potential leaks or risks.
- [ ] Define an observation and reporting system to detect threats and vulnerabilities in the infrastructure.
- [ ] Ensure that management participates in and is aware of the scope of the Information Security Management System (ISMS) and the associated risks.
- [ ] Ensure that employees are educated and aware of the scope of the Information Security Management System (ISMS) and the associated risks.
- [ ] Define roles and policies for vendors and educate them on the ISMS policies and how to handle data. Review their resilience periodically.
- [ ] Ensure a clear responsible, accountable and policy enforcer for management positions such as CTO and CIO.
- [ ] Ensure policies, documents and records, within the scope of both ISMS and ISO documentation, are updated according to technology evolution.

Processual

- [ ] Define an observation and reporting system to detect threats and vulnerabilities in the infrastructure.
- [ ] Define control points for predicative-alerts and points of evaluation for the amount of risk that they represent.
- [ ] Define clear functions for the organisation, and enforce that any member and element of the organisation follows the established policies.
- [ ] Ensure that management takes actions periodically on the evaluation of risk and simulation of risk.
- [ ] Enforce reporting capabilities within any member of the organisation. Educate on risk signal perception and evaluation.
- [ ] Make sure that incident response and business continuity plans are established and regularly updated.
- [ ] Reinstate verification procedures that are conducted monthly to ensure that all backups function as intended.

CW1

Assets

- [ ] Ensure a clear management action in protecting asset crownjewels as well inventory, infrastructure and products.
- [ ] Educate every member of the organisation to take action in protecting inventory, infrastructure and products.
- [ ] Develop systems that ensure risk-mitigation and risk control. Usage of AI is encourage to identify possible breaches in time.
- [ ] Log every possible action from any member of the organisation, and ensure a revision of logs periodically.
- [ ] MFA for everybody and EDR with email validation are a must nowadays. SPTT recognition is optional but ensure constant infrastructure monitoring and backup.
- [ ] Define infrastructure digital and physical switches that ensure disconnection in case of security breach.
- [ ] Ensure policies, documents and records, within the scope of both ISMS and ISO documentation, are updated according to technology evolution.

Third parties

- [ ] Conduct a thorough risk assessment of vendor systems, data access and handling practices, and contracts to ensure that they meet your organization's data security standards.
- [ ] Ensure that vendors comply with your organization's data handling policies by requiring them to undergo regular training on data security and compliance.
- [ ] Establish clear data breach notification and incident response protocols with vendors to minimize the impact of security incidents and breaches.
- [ ] Regularly review and audit vendor security practices and data handling processes to ensure that they remain compliant with your organization's security policies and regulatory requirements.

As cybersecurity threats continue to evolve, CISOs must be proactive in enforcing security policies to minimize risks to their organization's data and systems. Here are three insights into how a CISO can be more proactive rather than reactive when enforcing security policies within an organization:

Establish a Culture of Security Awareness: The first step towards proactive cybersecurity is to establish a culture of security awareness within the organization. CISOs can achieve this by regularly communicating the importance of cybersecurity to employees, educating them on safe computing practices, and providing them with the necessary tools and resources to identify and report security threats.

Conduct Regular Risk Assessments: CISOs should conduct regular risk assessments to identify potential vulnerabilities and security threats to the organization's data and systems. By identifying risks before they can be exploited, CISOs can implement preventive measures and minimize the impact of security incidents.

Implement Proactive Monitoring and Incident Response: CISOs should implement proactive monitoring and incident response measures to detect and respond to security incidents before they can cause significant damage. This includes the implementation of security monitoring tools, threat intelligence feeds, and incident response plans to detect and respond to potential security incidents. By implementing these measures, CISOs can minimize the impact of security incidents and protect their organization's data and systems from cyber threats.

Another key component of data security is access control. Organizations should implement strict access controls to ensure that only authorized personnel have access to sensitive information. This includes implementing multi-factor authentication, regularly reviewing access logs, and restricting access to only those who require it.

Regular monitoring and testing of the organization's security measures is also important. This includes conducting regular vulnerability assessments and penetration testing to identify any potential weaknesses in the organization's security infrastructure.

Ultimately, data security is everyone's responsibility. Every employee should be actively engaged in preventing data security incidents and protecting the organization's sensitive information. By staying informed, being vigilant, and following best practices, we can all play a part in ensuring the security of our organization's data.

CW1