Deloitte.

Stay ahead. Stay secure. Drive your business with ‘Cyber Asset Risk Management’

May 2024

Introduction

The digital landscape has undergone significant evolution over the past few years, driven by advancements in technology, changes in consumer behavior, and shifts in business paradigms. Organisations across various sectors are undergoing digital transformation initiatives to stay competitive in a rapidly evolving landscape. It has become more complex and interconnected, leading to increased cybersecurity threats and challenges across different industries.

The state of cybersecurity in today's business landscape:

1. **Increasing cyber threats**
   - Ransomware
   - Data breaches
   - Phishing
   - Supply chain vulnerabilities
   - Nation-state-sponsored attacks
2. **Regulatory compliance**
   - GDPR (General Data Protection Regulation)
   - CCPA (California Consumer Privacy Act)
   - PCI-DSS (Payment Card Industry Data Security Standard)
   - HIPAA (Health Insurance Portability and Accountability Act)
3. **Emerging technologies**
   - Cloud computing
   - Internet of Things (IoT)
   - Artificial Intelligence (AI)
   - Edge computing
4. **Ransomware epidemic**
   - Data encryption
   - Payment demands
   - Financial losses
   - Operational disruptions
5. **Supply chain risks**
   - Third-party vendor vulnerabilities
   - Software and services integrity compromises
6. **Remote work challenges**
   - Increased cybersecurity risks
   - Endpoint security needs
   - Secure remote access solutions
7. **Zero trust security**
   - Continuous identity verification
   - Strict access controls
   - Micro-segmentation
8. **Value of cyber assets**
   - Sensitive data protection
   - Intellectual property security
   - Business operations preservation
   - Customer trust maintenance
   - Competitive edge preservation

Today's cybersecurity business landscape is characterised by escalating cyber threats, supply chain risks, regulatory compliance requirements, and remote work challenges, prompting a need for a proactive cybersecurity posture.

Business challenges

In the realm of cybersecurity, businesses face a multitude of challenges. Here's an overview of cyber challenges across various industries:

Financial Services:

- **Data breaches:** Financial institutions are prime targets for cybercriminals seeking to steal sensitive financial data like credit card information and personal identities.
- **Ransomware:** Attackers may encrypt critical financial data and demand ransom for decryption.
- **Regulatory compliance:** Financial organisations must comply with stringent regulations such as PCI-DSS, GDPR, and industry-specific regulations like SOX (Sarbanes-Oxley Act).

Healthcare:

- **Data privacy:** Healthcare organisations store vast amounts of sensitive patient data, making them lucrative targets for data breaches.
- **Ransomware:** Hospitals and clinics are frequently targeted by ransomware attacks, disrupting operations and endangering patient care.
- **Compliance challenges:** Healthcare providers must comply with regulations such as HIPAA (Health Insurance Portability and Accountability Act), which mandate strict security measures for protecting patient information.

Government and Public Sector:

- **Cyber espionage:** Nation-states and other threat actors may target government agencies to steal sensitive information or disrupt critical infrastructure.
- **Supply chain attacks:** Governments rely on numerous suppliers for various services, making them vulnerable to supply chain attacks that compromise the integrity of software or hardware.
- **Critical infrastructure protection:** Attacks on critical infrastructure, such as power grids and transportation systems, can have severe consequences, including economic disruption and public safety risks.

Technology and IT Services:

- **Intellectual Property (IP) Theft:** Technology companies face threats from both cybercriminals seeking to steal valuable intellectual property and nation-states engaged in industrial espionage.
- **Supply chain attacks:** Technology companies rely on global supply chains for hardware and software components, making them vulnerable to supply chain attacks.
- **Data privacy concerns:** Tech firms often handle vast amounts of user data, raising concerns about privacy breaches and regulatory compliance.

Key challenge – Cyber assets

Cyber assets serve as a prime target for cybercriminals aiming to breach security, gain unauthorised network access, steal confidential data, and disrupt operations. These assets can take multiple forms such as internet-facing web applications, mobile applications, and APIs that help produce value for organisations, enabling the organisation to achieve business purposes.

Web applications

- Internet-facing websites are not immune to cyber-attacks. They are susceptible to various threats such as cross-site scripting (XSS), SQL injection, and DDoS attacks.
- Managing risks associated with the ever-growing web attack surface is crucial to enhance the security posture of the organisation.

Mobile applications

- Mobile applications often handle large amounts of sensitive information, making them attractive targets for cyber-attacks.
- It is essential to prioritise the security posture of mobile applications across various platforms such as Android, iOS, and hybrid applications.

Application programming interface

- APIs play a critical role in connecting multiple applications, but they can also pose security risks if left exposed without proper security measures.
- By implementing robust API security controls and conducting regular security assessments, organisations can ensure secure access to software functions and data through APIs.

The expanding threats to cyber assets have triggered a need for a robust cyber asset risk management program that can ensure continuous identification and remediation of threats.

Our services

With ongoing digital transformation and increased connectivity, safeguarding cyber assets and enhancing organisational visibility to manage cybersecurity risks are imperative. Cyber Asset Risk Management extends beyond traditional risk management boundaries, emphasising proactive and adaptable risk management to address regulatory compliance complexities and the rapid evolution of technology.

Our fully managed “Cyber Asset Risk Management” solution ensures continuous **identification, analysis, evaluation, prioritisation, treatment, and monitoring** of cyber assets. It enables a nuanced and responsive approach to cyber risk management, essential in today’s interconnected world. It facilitates service request initiation, monitors progress, and offers comprehensive metrics for quality control and continuous improvement.

With our solution, you can confidently ensure the security of your applications while delivering exceptional service to your customers.

Stages of our cyber risk services:

Identification

- **Define cyber assets:** Identify and classify all cyber assets within the organisation's infrastructure such as web applications, mobile applications, and application programming interfaces.
- **Inventory assets:** Create an inventory of cyber assets, documenting details such as asset type, location, ownership, criticality, and dependencies.
- **Evaluate assets:** Understand the functionality of the cyber asset, evaluate the sensitivity of the data being handled by the asset, determine a risk score, and select an appropriate assessment level.

Analysis

- **Threat assessment:** Assess potential threats and vulnerabilities to cyber assets in line with security standards such as OWASP top 10, considering factors such as the organisation's industry, regulatory requirements, threat landscape, and attack surface.
- **Vulnerability scanning:** Conduct vulnerability scans and assessments to identify weaknesses and security gaps in cyber assets, including software vulnerabilities, misconfigurations, and outdated systems.

Evaluation

- **Risk assessment:** Evaluate gaps, determine risks associated with each cyber asset, and provide recommendations to facilitate remediation.

Prioritisation

- **Risk prioritisation:** Prioritise cyber risks based on their severity and potential impact on business operations, and alignment with organisational objectives.

Treatment

- **Risk mitigation strategies:** Develop risk mitigation strategies and controls to reduce the likelihood and impact of identified cyber risks. This includes implementing technical controls and security best practices in line with industry standards and regulatory laws. Oversee risk remediation, grant approvals based on the assessment report, and identify post-launch checks.
- **Risk acceptance:** Document and communicate the risks that can't be immediately fixed and facilitate a risk acceptance strategy, consisting of the plan for remediation, along with the timelines. Ensure all business stakeholders are aligned.

Monitoring

- **Continuous monitoring:** Implement continuous monitoring practices to track changes to the cyber assets, assess the effectiveness of risk mitigation measures, and detect emerging threats or vulnerabilities via periodic vulnerability scans.
- **Key Performance Indicators (KPIs):** Define and track key performance indicators related to cyber asset risk management, such as vulnerability remediation rates, incident response times, and security posture improvements.

Key features of our services:

- Informed decision making
- Operational efficiency
- Compliance and regulations
- Dynamic risk assessments
- Real-time visibility
- Risk awareness
- Automation
- Performance management
- End-to-end support
- Collaboration

Cyber Asset Risk Management framework

A comprehensive framework for cyber asset risk management provides a structured approach to identify, assess, mitigate, and monitor risks associated with cyber assets within an organisation's infrastructure. Effective cyber asset risk management is not just a technical necessity; it is a crucial component of maintaining your reputation and trust with customers.

However, achieving and maintaining effective cyber asset risk management requires ongoing dedication. It is essential for organisations to continuously assess and mitigate cybersecurity risks and collaborate closely with stakeholders to ensure alignment and coordination in cybersecurity efforts.

Stages of our Cyber Asset Risk Management solution:

Initiation

- **Compile data:** Gather relevant information about the application, its infrastructure, functionality, and any previous security assessments.
- **Identify interested parties:** Determine stakeholders involved in the assessment, such as developers, security teams, project managers, and business owners.
- **Specify scope:** Define the scope of the assessment, including the boundaries, objectives, and assets to be evaluated.
- **Examine compliance standards:** Review relevant regulatory requirements, industry standards, and best practices to ensure compliance.
- **Utilise checklist:** Utilise a checklist or framework to systematically assess security controls and identify potential gaps.
- **Obtain pre-production environment information:** Gather details about the pre-production environment to facilitate security testing and analysis.

Assess

- **Infrastructure and functionality assessment:** Evaluate the application's infrastructure, architecture, and functionality to identify potential security vulnerabilities and weaknesses.
- **Fingerprinting methodologies:** Employ fingerprinting techniques to gather information about the application's technology stack, configurations, and potential attack surfaces.
- **Manual and automated testing:** Conduct both manual and automated security testing to assess the effectiveness of security controls and identify vulnerabilities.
- **Alignment with industry standards:** Evaluate the security controls against industry standards, frameworks, and best practices to ensure compliance and effectiveness.

Pre-launch

- **Collect evidence:** Document findings and evidence to support identified security gaps and vulnerabilities.
- **Gap evaluation:** Assess the severity and criticality of identified gaps and vulnerabilities based on their potential impact on the application and organisation.
- **Report to stakeholders:** Communicate findings and recommendations to relevant stakeholders, including management, developers, and security teams.
- **Initiate remediation plan:** Develop and implement a remediation plan to address identified security gaps and mitigate risks before the application's launch.

Implement

- **Control implementation:** Implement security controls and measures to mitigate identified risks and vulnerabilities.
- **Residual risk determination:** Assess the residual risk after implementing controls to determine the effectiveness of risk mitigation efforts.
- **Verification and testing:** Verify and test implemented controls to ensure they adequately address identified security risks and comply with security requirements.

Continuous monitoring

- **Post-launch activities:** Perform periodic vulnerability scans and security assessments on the production environment to identify and remediate any new vulnerabilities.
- **Fix existing vulnerabilities:** Address existing vulnerabilities and security gaps identified during the assessment and monitoring process.
- **Dashboard publication:** Publish monthly dashboards or reports to track security metrics, vulnerabilities, and remediation progress, enabling stakeholders to monitor the application's security posture and initiate timely remediation actions.

The benefits

- **Unique solution creation:** Customised solutions aligned with organisational environment, industry standards, and legal requirements for enhanced cybersecurity tailored to specific business needs and regulatory compliance.
- **Platform-neutral specialists:** Utilising specialists proficient across various platforms for simplified technology integration and seamless interoperability between systems.
- **Centralised asset inventory:** Maintaining a centralised inventory of assets ensures end-to-end traceability, enhancing visibility and management of cyber assets.
- **Governance framework:** Developing a prescriptive governance framework collaboratively with teams to identify, monitor, and remediate vulnerabilities, ensuring consistent and effective risk management practices.
- **Service request tracking:** Enabling initiation and monitoring of service requests across operational stages for continuous improvement and enhanced efficiency.
- **Automation for efficiency:** Identifying automation opportunities to streamline operations, reduce manual effort, minimise human error, and enhance productivity.
- **Continuous analysis and metrics:** Ongoing asset analysis, metric calculation, and dashboard generation for proactive monitoring, timely identification of non-compliant assets, and continuous improvement efforts.
- **Cost-saving:** Providing cost-effective risk management solutions compared to expensive penetration options.
- **Reputation and trust:** Safeguarding customer data to build trust and ensure long-term success.

Why choose Deloitte?

We're a worldwide leader in cyber risk management. Our services span the entirety of cyber risk management, leveraging extensive technological proficiency, wide-ranging industry insights, and a comprehensive array of solutions. Addressing every facet of cyber risk management, we're equipped to assist clients in navigating the intricate and evolving landscape characterised by emerging technologies and heightened connectivity.

In addition, we:

- Push the boundaries of cybersecurity risk strategy and create new avenues for innovation by partnering with global leaders.
- Develop new knowledge of cyber risk and upscale the industry by cultivating best-in-class expertise.
- Strengthen cyber risk standards for organisations worldwide by investing in cutting-edge technology.
- Make a bigger impact on our client's operations to drive progress by offering a comprehensive suite of solutions across strategy, implementation, and managed services.
- Leverage cutting-edge technology and renowned tools to stay ahead of emerging threats. Our proactive approach to security ensures that your systems are continuously monitored and protected against evolving cyber risks.

We offer you

- More than 1850 cyber practitioners across India.
- 17 years of providing cyber risk services.
- Three 365x24x7 Cyber Intelligence Centres spread across India.
- 650 certified professionals with a range of certifications, such as CISA, CISSP, CEH, CISM, and OSCP certifications.
- Cyber professionals trained on diverse range of vulnerability scanning tools such as Qualys, MobSF, NoName Security, Snyk, Veracode, and others.
- Robust vulnerability management strategies to proactively identify, prioritise, and remediate security vulnerabilities across your organisation's cyber assets, in line with the guidelines outlined by OWASP Top 10.

Connect with us

If you want to know more about cyber asset risk management, let's talk.

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Munjal Kamdar
Partner, Risk Advisory
Deloitte India
mkamdar@deloitte.com

Himanshu Surange
Partner, Risk Advisory
Deloitte India
hsurange@deloitte.com

Deloitte.