Cox Automotive, Inc.

Information Security Program Overview

Customer Use Only

January 2023

The following Overview provides information to customers of Cox Automotive, Inc. about the information security programs as of the date of this Overview for the following affiliates, including Dealer.com, Dealertrack (F&I, DMS, CMS, DDS), F&I Express, Esntial, VinSolutions, and xTime, as may be required by the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq. ("GLB Act"), and its implementing regulations. This Overview does not apply to any other Cox Automotive, Inc. affiliates.

Cox Automotive continues to undertake a comprehensive review of its security controls, including compensating controls, and may enhance its program and update this Overview as appropriate.

Compliance Program: Customer Systems

Information Security Program

- ☑ Documented, annually reviewed Information Security Policies and Program
- ☑ Dedicated Information Security staff with a CISO
- ☑ Periodic & annual program for security risk assessments
- ☑ Program to train all employees and contractors upon hire and annually thereafter, including role-based training
- ☑ Mature Incident Response program co-owned by Legal and Security
- ☑ Best in class EDR (Endpoint Detection and Response) solutions deployed on all user devices and servers

Third-Party Risk Program

- ☑ Documented and mature third-party risk management program
- ☑ Continuous monitoring enabled for critical third parties
- ☑ All service providers required to abide by applicable state and federal laws

Access Controls

- ☑ Multi-factor authentication is available for substantially all customer facing and backend systems
- ☑ System lock-out enabled to prevent brute-force attacks
- ☑ Robust Password requirements aligned with NIST guidance
- ☑ Access based on least privilege and need-to-know managed by policy and process

Application Security Controls

- ☑ All customer facing systems hosted in SOC2 certified data centers
- ☑ All website transmissions are encrypted over the Internet
- ☑ For backend file transfers, encryption capability is available for all endpoints
- ☑ All sensitive personal information encrypted at rest in storage
- ☑ Vulnerability management program implemented
- ☑ Weekly and monthly scanning implemented
- ☑ Annual independent third-party penetration testing
- ☑ 24x7 monitoring with SIEM implemented
- ☑ Secure data destruction and device decommissioning processes implemented
- ☑ Production and consumer data not permitted on test or non-production environments

Enterprise Risk and Security

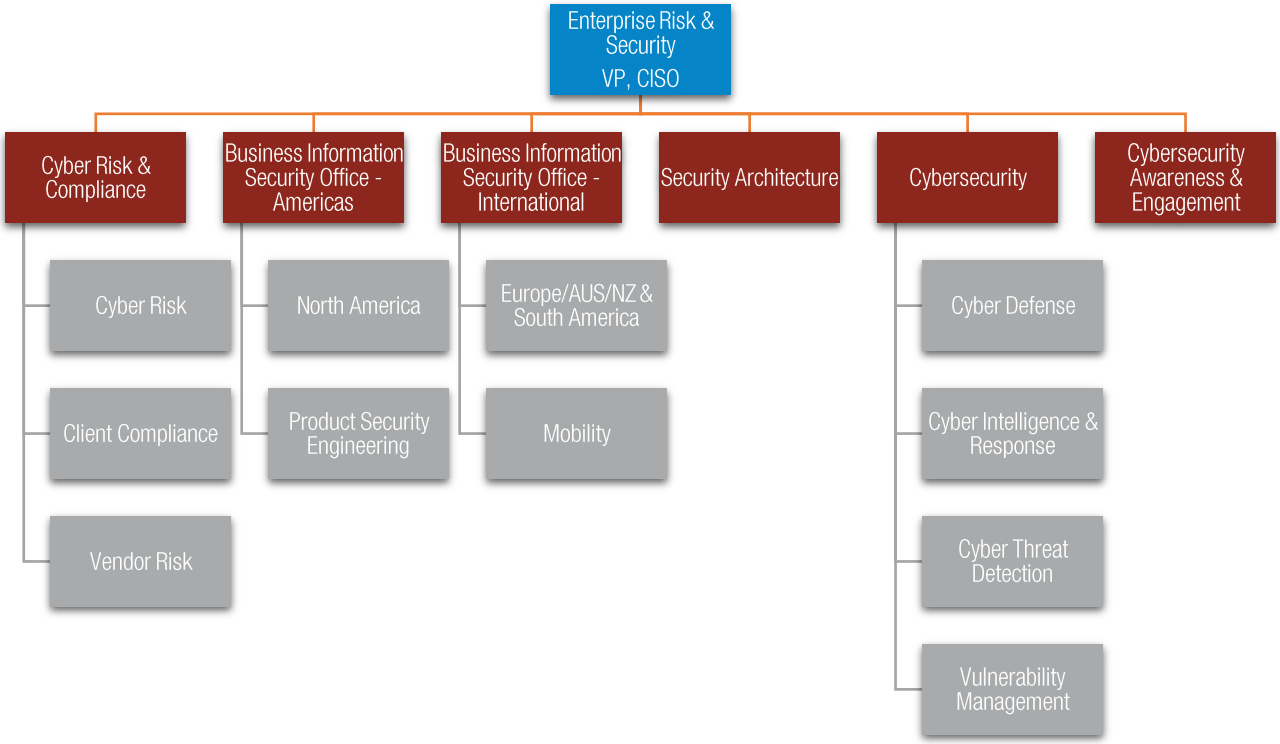
Enterprise Risk and Security (ERS), led by the Chief Information Security Officer (CISO), is responsible for defining, implementing, and executing Cox Automotive's Governance, Risk Management and Compliance (GRC) strategies. The objectives of the GRC program span all Brands under the Cox Automotive portfolio and ensures alignment with the overall business and strategic objectives.

Governance

Cox Automotive's Governance strategy establishes an organizational structure that defines ownership, assigns roles and responsibilities, designates decision-making authority, and ensures that the intended outcomes of the information security program are achieved. Additionally, information security policies and standards are established and maintained to support business objectives and reinforce ethical, legal, and risk mitigating behavior across the organization. Policies and standards are required to be documented, communicated, and reviewed periodically.

Enterprise Risk & Security Organization Chart

Enterprise Risk & Security's centralized organizational structure is aligned to meet Cox Automotive's business objectives. This high-level chart provides an outline of the allocation of information security roles and ownership.



Policy and Standards Management

Cox Automotive continuously assesses its business activities, responsibilities, and the external environment to identify the need for policy creation, revision, or termination. The creation or revision of a policy may be initiated by the business but must be formally approved by applicable functional leadership. Policy implementation and communications occur only after formal approval. Updating and maintaining policies is an ongoing process that includes the periodic review, revision, succession, or termination of a policy. At Cox Automotive, policies are reviewed at least annually.

Information Security Policy & Standards (Table of Contents provided to show comprehensiveness of policy)

Table of Contents

Information Security Policy & Standards (Table of Contents con't)

Information Security Risk Management

Cox Automotive has implemented Information Security Risk Management (ISRM) processes to ensure that risks to confidentiality, integrity, and availability are identified, analyzed, and maintained at acceptable levels. The Information Security Risk Management covers all Information Resources, whether managed or hosted internally or externally. The ISRM process is designed to establish an iterative approach for identifying, assessing, responding, mitigating, and reporting risks. Business Information Security Advisors (BISA), Information Technology (IT), Business Units, and Stakeholders are responsible for working with the Enterprise Risk and Compliance (ERC) team to implement the ISRM program, including remediation of identified risks in a timely manner.

The ISRM is comprised of the following processes outlined below.

Third-Party Risk Management

The Third-Party Risk Management Program is a core component of Cox Automotive's overall information security risk management strategy. The program is intended to maximize the benefits received from the third-party relationship, service or product, while simultaneously minimizing associated risks. We understand that third-party relationships play a key role in the success of an organization. But these relationships can also introduce substantial risk and need to be carefully managed. As the scale, scope, and complexity of these relationships and services increase, the related risks and the importance of effective third-party management proportionately increase in criticality to our organization.

Cox Automotive's robust risk management program includes due diligence in the selection of business partners and third parties as well as on-going monitoring activities. The third-party relationship is viewed holistically in the organization with the associated risk management processes executed in two distinct stages. The first is the initial onboarding and risk assessment of the new third-party provider which is embedded into the Supply Chain Management and Technology Business Management Office processes. The second is the ongoing monitoring and periodic risk assessments of the third-party providers which is managed by the Enterprise Risk & Security team.

Other key program elements include but are not limited to managing the relevant third parties in one central location, classifying the third party based on established risk criteria, contract management and review, and the tracking and remediation of risk areas.

Enterprise Change Management Overview

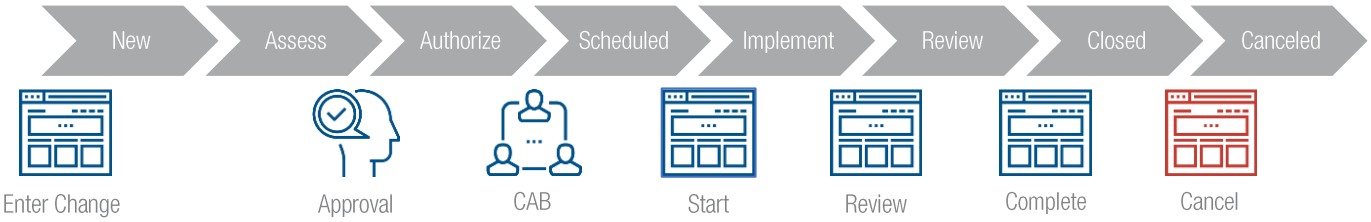
Overview

The change management process assesses, manages and communicates all changes in the production environment. This process helps to ensure services are stable, reliable, and able to change rapidly to meet evolving business requirements. Cox Automotive business units are moving to a single process and system of record for all changes across the enterprise. This process is owned by the Enterprise Operations Center (EOC).

Roles and Responsibilities

The EOC is also responsible for Systems Monitoring, Major Incident Management, Problem Management and Analytics.

Change Management Process Flow



Change Advisory Board (CAB) Meeting Schedule

The Change Advisory Board meets at least once weekly to review changes. CAB agenda reports are sent 24 hours prior to the CAB meeting and the approved changes report is sent 24 hours after the CAB meeting for all non-Dealertrack companies. Dealertrack approved changes are sent daily.

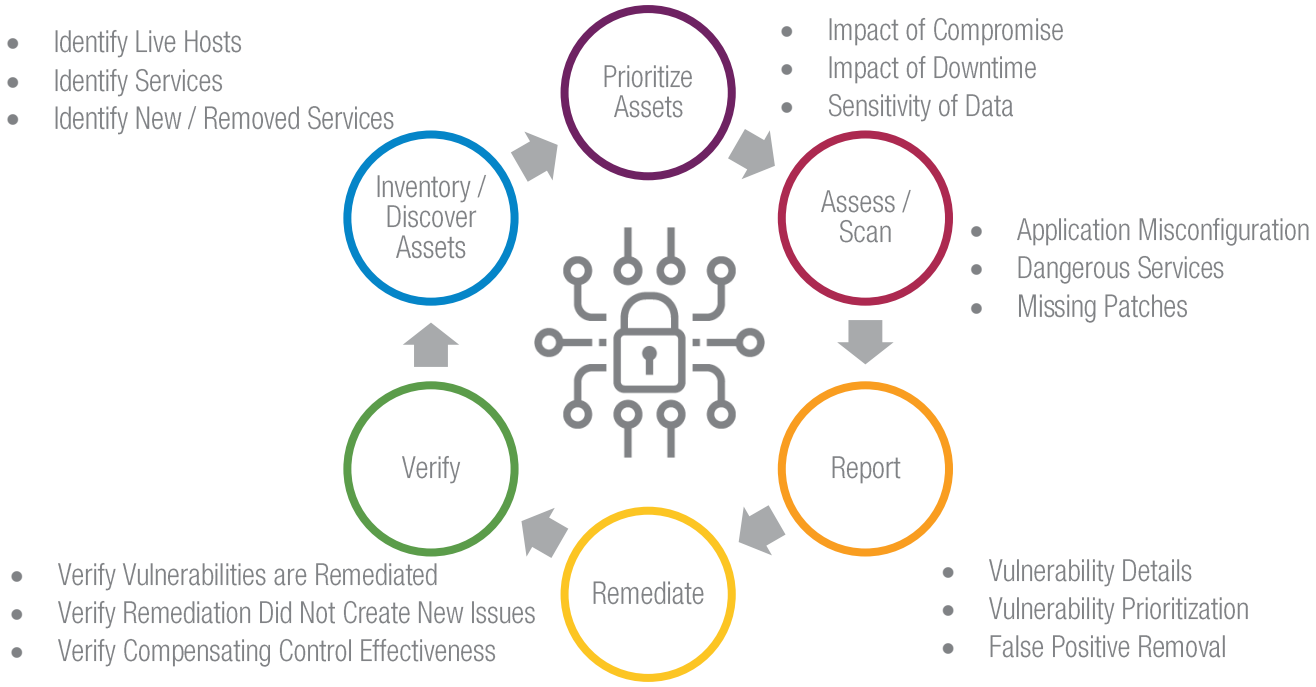
Vulnerability Management Program Overview

One of the many challenges faced by Enterprise Risk & Security is the ongoing protection of Cox Automotive's assets from today's ever evolving cyber threats. As an organization, it is critical that we can identify, analyze, evaluate and remediate cyber risks before they can be exploited and potentially cause reputational damage or loss to confidentiality, etc.

Our Vulnerability Management Program is an essential component of our overall security program. It allows us to plan for and determine the appropriate implementation of controls and processes to identify vulnerabilities in Cox Automotive's operating systems, applications, mobile devices, cloud resources, and network devices. It ensures that assets and applications deployed are tested and protected from possible exploitation.

Vulnerability management is not a one-time task—it needs to be an ongoing process to be successful.

At Cox Automotive we've adopted a six-step vulnerability management process to ensure the ongoing protection of our network and systems from ever present and evolving cyber threats.



Network Vulnerability Assessment

Cox Automotive's Enterprise & Security Vulnerability Management Program includes having external and internal network vulnerability assessments performed on at least bi-weekly to identify security vulnerabilities. There is a continuous improvement process for reviewing and implementing additional security measures to mitigate future exposures of or vulnerabilities to our systems.

Application Vulnerability Assessment

Internet applications are susceptible to application vulnerabilities. Without proper precautions, use of a Web-based application can expose systems and users to vulnerabilities such as Cross Site Scripting (XSS) and SQL Injection attacks.

Cox Automotive utilizes both static code scans and dynamic scans for application testing. These testing methods provide us with vulnerability reports and remediation recommendations so that Cox Automotive's Enterprise Risk & Security can partner with Application Development teams to review and remediate findings that are discovered prior to being deployed to production environments.

Penetration Testing

Cox Automotive periodically leverages independent, third-parties to conduct network and application penetration testing. The penetration tests mimic real-world threats to demonstrate a potential for loss. Prior to testing, the scope of the engagement and penetration testing approach are documented. At the completion of the penetration test, reporting documentation is provided that includes:

- Detailed results of the testing performed;
- What the results indicate; and
- Corrective action/remediation recommendations

Identified findings resulting from the penetration test are entered into the risk register and tracked for remediation.

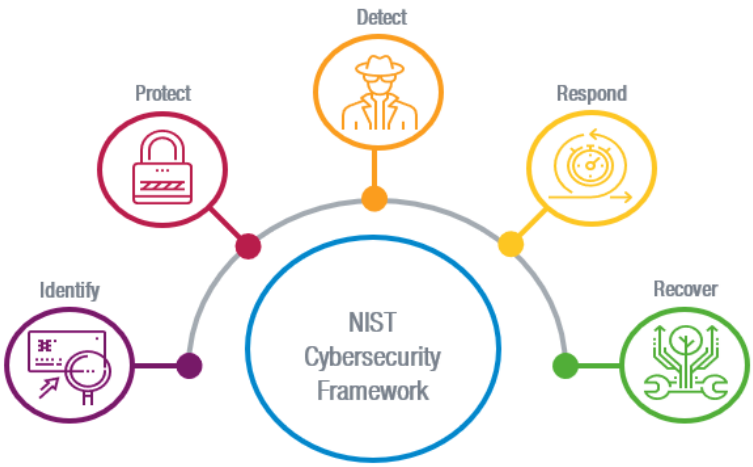
Cybersecurity Program Overview

As Cyber threats continue to rise and become more sophisticated, Cox Automotive has implemented a comprehensive Cybersecurity program to protect our services and information assets.

Cox Automotive's Cybersecurity program follows industry best practices by aligning to NIST Cybersecurity framework to protect the organization. We follow an iterative and continuous improvement process in advancing our program to be proactive in addressing threats that could impact our services we provide to our customers.

Cox Automotive has implemented best of breed Cybersecurity products on our systems, Customer applications, network, and email to provide a holistic Cybersecurity coverage across all threat vectors. Furthermore, to proactively identify and respond to threats that may impact Cox Automotive we have an advanced threat intelligence program. We receive threat intelligence feeds that enrich our security systems from open source, commercial, and government agencies.

From a Cybersecurity operations perspective, all internal and external threats identified from in-house or commercial tools are centralized within a SIEM (Security Information and Event Management) System and are monitored 24X7 by our MSSP (Managed Security Service Provider) and triaged appropriately. In addition, automated processes have been established to reduce the time to detect and respond to Cyber threats.



Malware Protection

Cox Automotive has implemented next generation Artificial Intelligence powered Anti-Malware solution to protect its remote, on-premise, and cloud-based systems against malware and ransomware. It uses behavior-based indicators, exploit blocking and threat intelligence to prevent fileless and malware attacks on the corporate systems. Endpoint security of the corporate systems are centrally managed by the corporate Cybersecurity team and the anti-malware platform is monitored on a 24/7 basis.

User Endpoint Security and Protections

Cox Automotive has a dedicated engineering team responsible for managing user endpoint devices (Desktops, Laptops, Mobile devices, etc.). These devices are secured and centrally managed with enterprise solutions like Intune MDM, Symantec DLP, CrowdStrike EDR, BitLocker encryption, etc.

Data Security Incident Response Program Overview (Table of Contents provided to show comprehensiveness of program)

Data Security Incident Response Program Overview

Contents

COX AUTOMOTIVE™

Business Continuity and Disaster Recovery Overview (Table of Contents provided to show comprehensiveness of program)

Disaster Recovery Management Program Overview

Contents

COX AUTOMOTIVE™

1

Compliance

ERS plays an integral party in ensuring that Cox Automotive sustains a culture and documentation that encourages ethical conduct and a commitment to complying with laws and regulations, including regularly updating the Code of Conduct and related policies. This is achieved by continuously monitoring benchmarks and providing education and awareness to drive an ethical culture.

Contractual and Regulatory

Cox Automotive is committed to conducting its business activities lawfully and in a manner that is consistent with its contractual obligations. ERS plays a role in reviewing contractual agreements for relevant security language and ensures that those obligations are met.

As the regulatory landscape is always evolving, ERS consistently reviews new and existing laws and regulations to identify regulatory risks and ensure they are responded to, when needed.

Internal Controls Governance

Cox Automotive's Internal Controls Governance (ICG) team partners with stakeholders to provide control and risk guidance, perform control and process assessments, and provide impactful recommendations. This team provides the following services: Financial Controls Governance, Compliance Support, Enterprise Risk Management, and Value-Add Projects

Hosting Systems

Cox Automotive leverages a mix of colocation data centers and cloud service providers for corporate systems. As a provider of critical services, these vendors are continuously monitored for compliance and assessed annually as part of our Third Party Risk Assessment program.

QTS Colocation Data Center (Suwanee)

QTS is a leading provider of data center solutions to the world’s largest and most sophisticated hyperscale technology companies, enterprises and government agencies. QTS operates 24 data centers located throughout the United States, Canada and Europe and independently audited for compliance and is certified and accredited for SOC 1, SOC 2, HITRUST, PCI DSS, FISMA, ISO 27001.

Switch Colocation Data Center (Las Vegas)

Switch operates highly efficient multi-tenant facilities that hosts servers and storage for many of the world's leading technology companies, including more than 40 cloud computing companies and a dense concentration of network carriers. Certifications for this location include SSAE-16 Type 1, ISO 27001, HIPAA, PCI-DSS, FISMA, FedRAMP, NIST 800-53, SOC 1, SOC 2, SOC 3, SSAE-18.

Cloud Service Providers

Cox Automotive leverages Cloud Service Providers (CSP), Amazon Web Services (AWS), and Oracle Cloud Infrastructure (OCI) for benefits such as scalability, flexibility, and redundancy. The approach to security with the CSP is a shared responsibility model between the CSP and our company. In this model, the CSP operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates and Cox Automotive is responsible for the guest operating system (including updates and security patches). Certifications for AWS and OCI include CSA, ISO 27001, HIPAA, PCI-DSS, FIPS, FISMA, FedRAMP, SOC 1, SOC 2, SOC 3.

Physical Security Program Overview

Visitor Access

Upon arrival at a Cox facility, visitors are required to check-in. Visitors are required to provide their name, company, purpose and duration of visit. At check-in, every visitor is given a badge. The badge displays the visitor's name. This visitor's badge must be worn at all times. All visitors must be accompanied by the team member(s) they are visiting for the duration of their stay.

Identification and Badges

Each Cox facility should require the display of identification badges by all persons while on company property, to include visitors, vendors and contractors. Each badge should be visually distinctive by color, with separate templates for Employees, Contractors and Vendors. Badges should be tracked and audited for lost and/or turned in upon separation from the company.

Physical Access Control

Cox facilities utilize an electronic access control (EAC) with real-time monitoring applications, report generation capabilities and compatibility with Cox's program card/photo ID/EAC badge system. In some smaller facilities evaluated as low risk, key controls (Restricted duplication manufactured key and issuance process) and/or cypher locks are acceptable.

Closed Circuit Television (CCTV)

Cox CCTV system includes the deployment of digital camera systems with digital video recording for all designated ingress/egress points and areas of criticality with archive video stored for a minimum of 30-90 days depending on facility type, camera placements that provide proper field of views and resolution to ensure appropriate image identification, and remote viewing and event driven programming. In some smaller facilities evaluated as low risk, no cameras are required.

People Solutions Security

Background Checks & Screening

Cox Automotive's onboarding, transfer, and separation practices apply to all full-time and part-time employees, as well as contractors. After receiving and accepting a contingent offer of employment, applicants are required to complete a thorough pre-employment background check and drug screen.

- Background Checks
- Seven Year Criminal History Check (Federal, Statewide, and County)
- Nationwide Sex Offender Check
- Verified Watch List (Includes OFAC)

Drug Screening

- Five-Panel Drug Test

Additional screening may be necessary based on the applicant's job duties. These include:

- Education Verification
- Previous Employment Verification
- Motor Vehicle Record Check
- Credit History Check

*Some contractual obligations may require business units to impose additional controls that may exceed requirements above.

Acceptable Use Policy

At onboarding, all employees and contractors are provided the employee handbook that outlines the acceptable (and prohibited) use of Cox Automotive's information resources and devices. Violations of Acceptable Use is subject to corrective action up to and including separation from employment.

Information Security Awareness, Education & Training

At Cox Automotive we're focused on building a security-aware culture to enable employees in understanding the risks in using today's technology and how to effectively recognize, respond, and defend against today's cyber threats, both at work and at home. The primary purpose of an effective information security training and awareness program is to establish and sustain an appropriate level of protection for Cox Automotive's information resources by increasing team members' awareness of their information security responsibilities. Specific objectives of this program include:

- Improving awareness of the need to protect Cox Automotive information resources;
- Ensuring that employees clearly understand their responsibilities for protecting Cox Automotive information resources;
- Ensuring that users are knowledgeable about the Cox Automotive information security policies and standards and develop skills and knowledge so they can perform their jobs securely.

ERS conducts Security Awareness Training upon hire and subsequently at least annually through interactive, hands-on exercises and knowledge assessments. In addition to annual training, reinforcement training such as newsletters, email messages, digital signage, posters, webcasts and other means are used by ERS. Team members are also encouraged to visit ERS' Security Awareness intranet site, where additional security best practices are guidance documents can be assessed. ERS leverages SANS for training and education content. SANS Security Awareness, a division of the SANS Institute, provides organizations with a complete and comprehensive security awareness solution Security Awareness Training Overview.