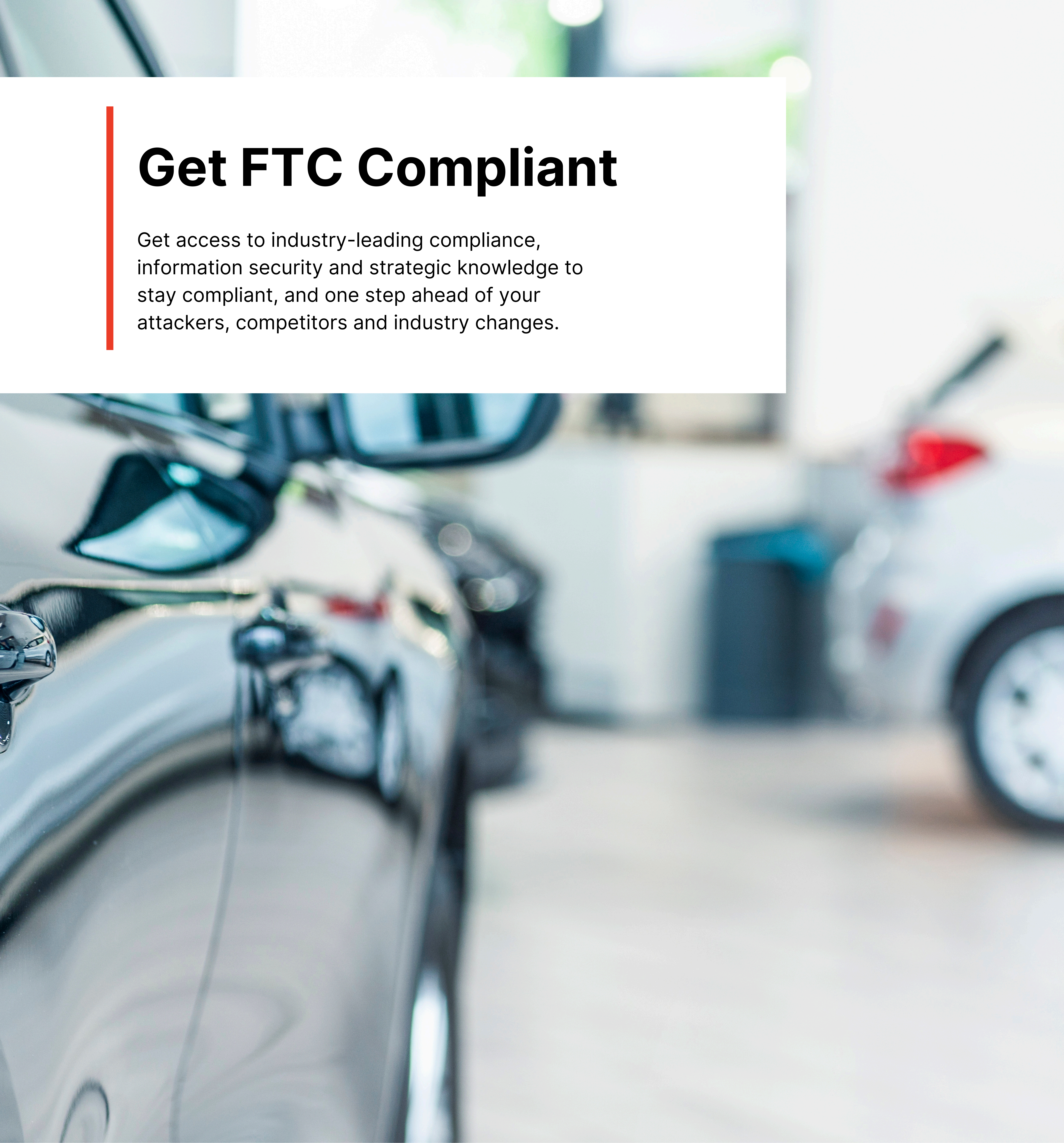
# Get FTC Compliant

Get access to industry-leading compliance, information security and strategic knowledge to stay compliant, and one step ahead of your attackers, competitors and industry changes.



subrosa

# What you need to know

Changes to the FTC's safeguards ruling now includes certain car dealerships among organization's covered by the rule, and categorizes them as financial services providers or financial advisors.

The FTC’s rule requires detailed procedures and specific criteria that auto dealers must implement to provide better protection and to curb data breaches and cyberattacks that could jeopardize sensitive customer data.

If you offer lease or financing agreements, you must abide by the ruling.

## NONCOMPLIANCE FINES CAN EXCEED $42,000 PER DAY

# Meet SubRosa

**Prepare for cyber incidents. Train your workforce. Respond to threats.**

SubRosa delivers unified FTC compliance, cyber risk solutions and services to help you achieve and maintain compliance with the FTC's ruling

We provide solutions to help you manage your entire risk and vulnerability landscape, from small dealerships to large enterprises.

## FTC Compliance Solutions.

RESPONSIBLE PERSON

### Hassle-free compliance

We save you on resources by handling the responsible person designation.

DOCUMENTED INFOSEC PROGRAM

### Proactively prepare.

A formally written information security program, updated at least annually.

CYBER ATTACK READINESS

### Proactively prepare.

A suite of services to help you prepare for cyber attacks.

RISK AND COMPLIANCE

### Know your organization.

Services to help you manage risk, and maintain regulatory compliance.

INCIDENT RESPONSE

### Respond to attacks.

Detect and prepare for incidents in real time.

INTEGRATED SOLUTIONS

### Leverage smart technology.

Leverage intelligent technology to gain full insights into your network and applications.

# Powerful expertise. Practical costs.

## Proactive Security.

### Cyber Attack Readiness

Prepare for a cyber attack with a range of proactive services.

### Social Engineering

Identify vulnerabilities in your procedures and personnel.

### Managed SOC

Gain unparalleled visibility into who is attacking your infrastructure.

### Risk & Compliance

Enhance confidence that your processes address current risks.

## Reactive Security.

### Incident Response

SubRosa's incident response team leverage real-world expertise, industry-leading technology and extensive threat intelligence to analyze and respond to a multitude of incidents, regardless of your organization's size.

### Computer Forensics Services

SubRosa's computer forensics experts can assist you with the most difficult and sensitive investigative or litigation issues requiring electronic evidence or data preservation.

PROACTIVELY PREPARE FOR CYBER ATTACKS

# Cyber Attack Readiness

Prepare for a cyber attack with a range of services from simulated attacks, vulnerability management to social engineering.

## Identify avenues of attack.

Cyber attack readiness is a fundamental cybersecurity service set for organizations of all sizes. Cyber criminals are attacking your networks, applications and people on a daily basis. Statistically speaking, almost every organization will have an attempted attack made against them, whether they realize it or not.

### NETWORK PENETRATION TESTING

Identify & Exploit Vulnerabilities. Simulate Attacks. Remediate and Protect Your Critical Network Assets with Network Penetration Testing.

### APPLICATION SECURITY TESTING

Static and dynamic app testing will identify vulnerabilities in your web applications that could lead to unauthorized data exposure.

### RED TEAM ASSESSMENTS

Red team assessments test your organization’s already established cybersecurity program and your team’s response and cyber attack readiness state.

### VULNERABILITY ASSESSMENTS

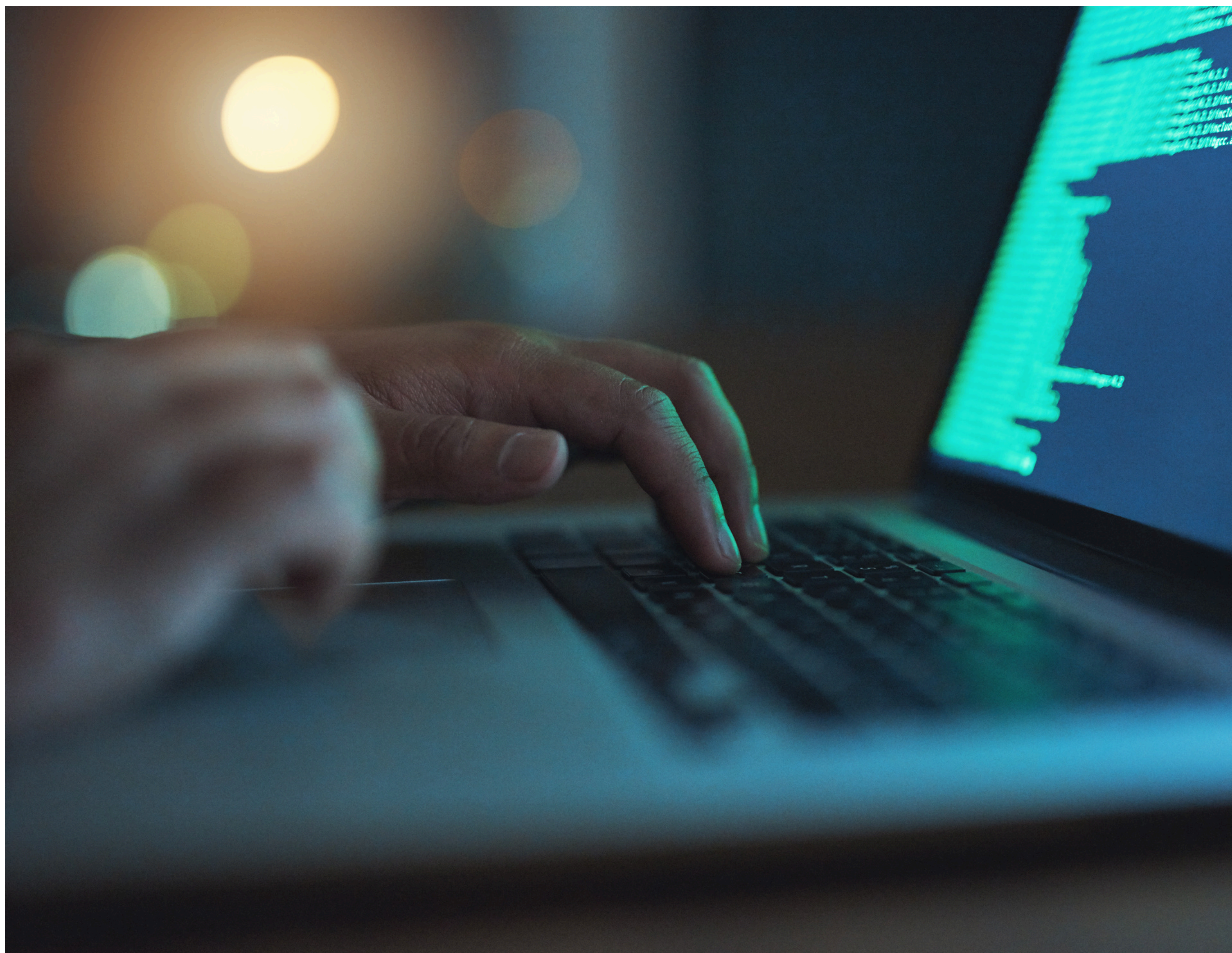
Vulnerability assessments will enable you to manage your vulnerability landscape with automated and manual vulnerability scanning and verification.

### SOCIAL ENGINEERING

Social Engineering will identify vulnerabilities in your personnel and test the effectiveness of your security awareness training.

### PHYSICAL PENETRATION TESTING

Physical penetration testing assesses the physical security controls of your locations, data centers and critical infrastructure.



MANAGE RISK AND MAINTAIN REGULATORY AND CONTRACTUAL COMPLIANCE

# Governance, Risk and Compliance

Eliminate holes in your company cyber security defenses to maintain the robustness of your essential information systems, and enhance confidence that your systems and processes address the current risks and industry standards.

As you manage the pressures of digitalization, new technologies, legislation, and the shifting risk and threat landscape at an accelerated pace, unique risks and cyber vulnerabilities that were previously unthinkable have become the commonplace. The good news: we can plan to fast adjust to these changes and take steps to guard against the risks.

### COMPLIANCE ASSESSMENTS

Achieve and maintain compliance with a wide range of industry frameworks and regulations.

### CYBERSECURITY MATURITY ASSESSMENTS

Assess your cyber program maturity level and pave the way for program improvements.

### CYBER AUDIT PREPARATION

Plan and prepare for audit and certification with audit preparation services.

### THIRD PARTY ASSURANCE

Assess and manage enterprise and cyber risks associated with your supply chain and third parties.

TIMELY, COST EFFECTIVE RESPONSE TO CYBER INCIDENTS

# Incident Response

Security incidents can cripple an organization's operations in a matter of minutes. If an incident is not responded to in a timely, professional manner, costs can spiral and irreparable damage can occur.

Failure to properly and efficiently manage a cyber incident can be drastically more costly for an organization than the actual incident itself. This presents resource-strapped IT executives with an increasingly burdensome challenge.

## Incident response services.

### COMPROMISE ASSESSMENT

Identify past and present attacker activity in your environment. Use the results to drive improvements to your incident response program.

### READINESS ASSESSMENT

Test your ability to respond to, manage and mitigate an incident from a wide array of attackers and attack types.

### INCIDENT RESPONSE TRAINING

Train stakeholders and incident response personnel to better prepare them for live incident response requirements.

### MANAGED INCIDENT RESPONSE

Bolster your incident response capabilities with a team on standby, ready to assist with incident response at a moments notice.

## Engagement models.

### PROACTIVE INCIDENT RESPONSE

Detect incidents in real time. Prepare for incident response through training and workshops.

### EMERGENCY INCIDENT RESPONSE

Respond to incidents post-discovery and engage SubRosa's cyber incident response and forensics team to assist.

### THREAT RESEARCH AND DEVELOPMENT

Research and analysis of emerging and existing threats to help proactively counter new threats, as they emerge.

### INCIDENT RESPONSE RETAINER

Retain industry-leading incident response experts, reducing the impact of incidents and enable quick, cost-effective response.

# Our Company

We deliver cutting edge security technology solutions and services to our Clients so that they are prepared to tackle the ever growing cyber threat. Through the SubRosa Unified Risk Platform, we deliver threat intelligence, security controls validation and incident alerting and response. We employ and partner with some of the leading risk and security experts in the industry, enabling us to deliver effective services and software solutions to our clients of all sizes, across the globe.

More resources available at: https://subrosacyber.com

**SubRosa**
2000 Auburn Dr
Ste 200 #366
Beachwood OH
44122
888.893.1983
info@subrosacyber.com

Since 2017 SubRosa proudly delivers cyber risk advisory and related services to public, private and government clients.

This brochure is to be used as a reference for general information only, and no content contained herein is designed to provide cyber risk professional advice or services.