CYBER SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

Shelter from the Storm

Minimise the attack surface of your supply chain

ILLUMINATE THE BLIND SPOTS IN YOUR SUPPLY CHAIN

The vast majority of breaches today are sourced to a “trusted” connection – an unfortunate fact. Consequently, the security integrity of 3rd party suppliers connected to your systems and processing your information assets are essential to the security of your organisation. Your business systems are only as secure as those systems connected to them. This simple logic is often overlooked.

Cost-effectively identify, minimise & manage the cyber security threats to your supply chain.

Risk Crew’s Cyber Supply Chain Risk Management (C-SCRM) Service is comprised of a proven process for identifying, assessing and mitigating cyber risks associated with the complex connected nature of the extended chain of your product and service suppliers.

It encompasses the entire supplier lifespan from “on-boarding” through service delivery (or product provision) to “off-boarding” as security threats and vulnerabilities change with each step depending on the associated activity and connectivity.

Simply put, a one-size-fits-all cyber risk management approach does not work. Our service ensures each supplier is subjected to an individual assessment – to ensure they meet your business’ security governance risk and compliance requirements and operate within your risk appetite and tolerance. This is no easy challenge, but we’ve got you covered.

SERVICE COMPONENTS

Our pragmatic, cost-effective and scalable solution is fully customisable to meet your specific risk objectives. The service can be designed and deployed within your existing business' supplier management processes or platforms. or automated and fully outsourced to Risk Crew for management.

The methodology is comprised of seven simple components:

Supplier On-Boarding

We begin the engagement by establishing the definition of a "Supplier," as this is often inconsistent across the business and can result in unidentified 3rd party services and connections going unaddressed. Next, we draft a C-SCRM plan for your business' governance framework that aligns with your risk appetite and tolerance objectives.

Risk Crew will then assess and align your current information asset classification scheme to appropriate the service level agreement language to include in applicable supplier agreements. This ensures that security requirements are understood by each party and contractually agreed upon during on-boarding.

Cyber Risk Triage

Risk Crew designs and deploys a supply chain risk triage portal based on the volume and sensitivity of the business' information assets that the supplier's process, stores or transmits on your behalf – along with specific connectivity and compliance requirements such as DPA, GDPR or the PCI DSS. For this, we utilise our proprietary 3PA Triage™ software solution. Once deployed, the model will quickly and easily segment your suppliers into risk categories of Low, Medium or High to prioritise the risk management process – giving a clear risk-driven view of your supply chain.

Automated Risk Assessments

Once triaged into applicable cyber risk categories (Low, Medium or High), suppliers are directed to complete a risk assessment questionnaire that is appropriate to their risk profile on the 3PA™ software platform. After questionnaires are complete, you will knowledgeably align specific risk assessment criteria to each supplier across the chain based on their potential risk to your systems and business information assets. The questionnaire is designed to identify and document the existing "inherent" risks associated with each supplier's current security controls. This tailored approach is important because when it comes to risk, one size does not fit all.

FULLY CUSTOMISABLE

The Risk Crew C-SCRM process can be delivered manually for your business to host in its current supplier management platform or through our fully automated 3PA and 3PA™ and hosted software solutions – you choose based on what suits your resources.

Prioritised Risk Remediation

Now that explicit “inherent” risks are identified for each supplier, you can assign specific actions to supplement or enhance existing security controls and reduce those risks to a level within your business’ risk appetite and tolerance. Supplier-specific risk-reduction activities are tracked through remediation and their “residual” risk status is logged for annual review. Key performance indicators (KPIs) are identified and collected throughout the process to verify overall risk reduction.

Security Testing

Throughout the engagement, Risk Crew conducts routine security testing to ensure the effectiveness of controls the supplier has implemented to secure your information assets and connectivity to your systems. Risk Crew will scope and conduct routine security testing of the supplier’s systems applicable to their residual risk profile and the technology platform processing, storing or transmitting your information assets such as web application, network, API, cloud or IoT. Bespoke control testing = bespoke cyber risk management.

Monitoring & Mentoring

Once the process is implemented, there is still work to be done. Risk Crew strongly believes that suppliers need continual monitoring and mentoring to ensure their understanding and correct implementation of the controls required to protect your information assets and their connectivity to your systems. The Risk Crew C-SCRM solution includes a supplier “helpline“ to answer any specific questions that may arise and provide best practice advice when needed. It also includes daily CERT alerts and monthly cyber security bulletins to keep suppliers apprised of current threats and vulnerabilities. We do this because we believe that education is the silver bullet.

Supplier Off-Boarding

Finally, it’s not over until it’s over. One of the most important (and overlooked) steps in any supply chain risk management lifecycle is the “goodbye”. The Risk Crew C-SCRM process includes detailed contract exit requirements from data retrieval or destruction to verifying termination of supplier connectivity to business systems. Requirements are mapped to specific existing business process to ensure their execution and the secure off-boarding of your supplier. This simple follow-through will dramatically decrease the chances of an accidental breach.

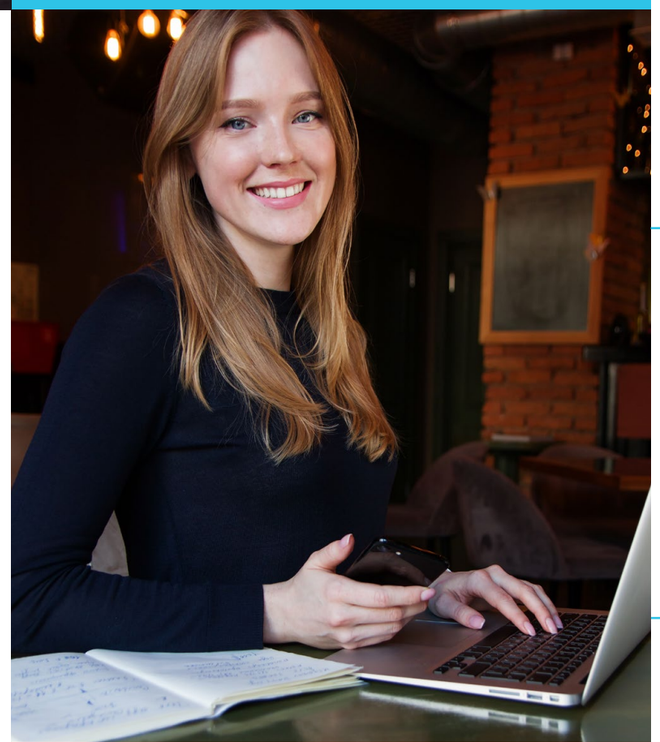
THE BENEFITS

- Today, everything is connected to everything. Therefore, businesses can no longer solely focus their cyber risk strategy only on protecting their internal infrastructures. Serious threat actors seek to exploit the less protected threat vectors provided by suppliers to their more cyber mature target. They bypass more mature cyber controls and exploit the weakest link in the chain. The risk is real and substantial.

- The Risk Crew C-SCRM service delivers a comprehensive and cost-effective solution for identifying, minimising and managing risk. Additionally, it provides metrics to calculate the return on your investment. It delivers risk transparency, liability and accountability for each supplier in your chain. It doesn't get any better than that.

WHY CHOOSE RISK CREW?

Our professionals possess over 20 years of experience in designing and delivering effective cyber supply chain risk management solutions. Our seasoned information security governance, risk and compliance consultants implement proven methodologies for documenting, assessing and remediating the cyber security risks to the information in your supply chain.



We like to help. It's what we do.

WHAT OUR CUSTOMER'S SAY

"Once again, Risk Crew impressed our Board (and made me look like a star). Well done."

Technology Industry Customer

"The simplicity of the solution was both powerful and effective. The portal platform is extremely intuitive and easy to use. Outstanding. "

Housing Industry Customer

"Excellent, professional and helpful service provided and great communication - I am glad we chose Risk Crew and look forward to working with you moving forward!"

Security Industry Customer

"A very positive experience. Risk Crew staff were friendly and professional throughout the engagement, keeping me informed and addressing all concerns in a timely manner. I won't hesitate to recommend Risk Crew or use them for future engagements."

Ultilities Industry Customer

Wow! Simple and really effective. Something the whole business easily understood and could get behind."

Finance Industry Customer

For effective cyber supply chain risk management – turn to the right crew, Risk Crew.

ABOUT RISK CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

Contact us for more information

+44 (0) 20 3653 1234

riskcrew.com

info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom