QUANTUM EVOLVE

Business & Cybersecurity Resilience Consultancy

Defending the Supply Chain Frontlines

A Tactical Guide to Third-Party Risk Management

www.quantum-evolve.com

© 2024 Quantum Evolve Limited

Why Should I Care About Third-Party Risks?

In the war against data breaches and supply chain disruptions, Third-Party Risk Management serves as your first battalion to defend against the enemies within.

It's key to your organisation's security as it helps to protect from the associated risks third-party vendors present.

Failure to effectively assess your supply chain exposes your organisation to potential data breaches and supply chain attacks.

This white paper, laden with a touch of humour, aims to elucidate the concept of Third-Party Risk Management and the myriad of risks it protects against.

It's important to stay vigilant, as third-party risks are now at the forefront of organisational threats.

"The supply chain stuff is really tricky"
- Elon Musk

© 2024 Quantum Evolve Limited

Know Thy Enemy

Organisations often have an obscured view of the risks that suppliers and other third-parties pose to their operations, reputation and bottom line.

Complex supply chains and outsourcing arrangements can hinder your ability to spot lax cybersecurity controls, logistical vulnerabilities or unethical behaviour among subcontractors and fourth, fifth and nth parties (suppliers of suppliers and so on).

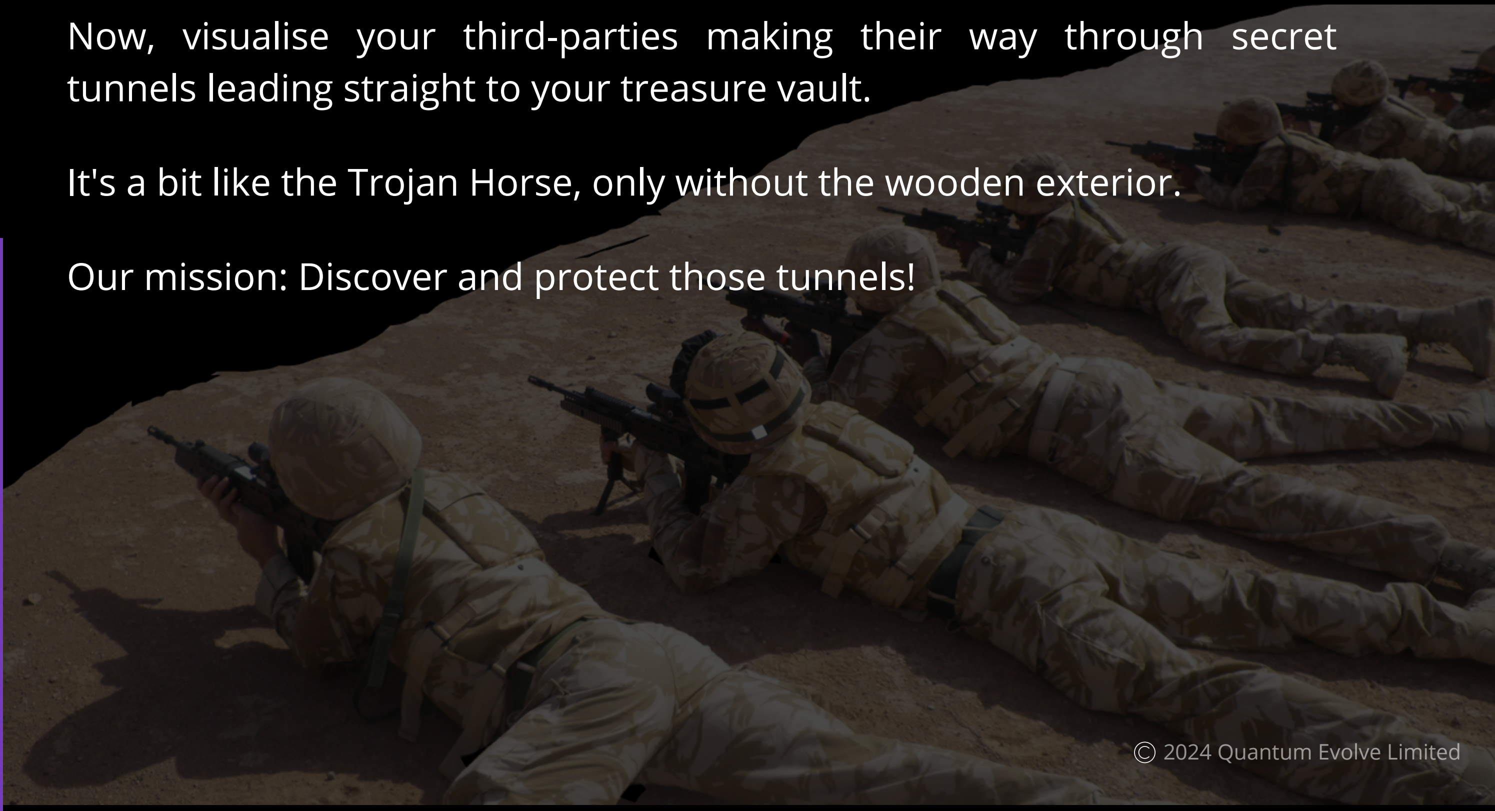
Let’s put it a different way.

Imagine that your organisation is a fortress and your data and supply chain secrets are locked up behind robust walls.

Now, visualise your third-parties making their way through secret tunnels leading straight to your treasure vault.

It's a bit like the Trojan Horse, only without the wooden exterior.

Our mission: Discover and protect those tunnels!



© 2024 Quantum Evolve Limited

Third-Party Risk Management: The Iron Shield

"A wise human would have an understanding of the supply chain and how the pieces fit together. But it's against our nature to think about it."
- Paolo Bacigalupi

Most organisations rely on outsourcing to handle at least some aspects of their day-to-day operations; as such the first line of defence is understanding what you're up against and third-party risk should be front of mind.

This is particularly true given the increasing number of security breaches that are arising from third-party relationships.

Despite the numerous risks that arise from these relationships, many organisations still do not manage third-party risks as diligently as internal ones.

Think of it as a crucial intelligence operation to weed out the spies and moles within your ranks.

© 2024 Quantum Evolve Limited

Failure to manage these risks can leave you exposed to regulatory action, financial exposure, litigation, reputational damage, and impair your organisation's ability to gain new, or service existing customers.

Supply chain attacks can devastate your business

According to the 2022 Cost of a Data Breach Report by IBM, the average cost of a data breach alone was $4.35 million.

However, with the right solutions, you can mitigate against the risks, and reduce the financial exposure to your organisation.

© 2024 Quantum Evolve Limited

Strategic Directive

To protect those aforementioned tunnels within Europe, the European Parliament has updated the Network and Information Security Directive (NIS). ALL EU member states will HAVE TO COMPLY with NIS 2 by 17 October 2024.

Building on the original mission manual, NIS 2 covers specific cybersecurity strategies that need to be followed, and informs you to establish competent authorities as well as implementing incident reporting mechanisms.

The European Parliament's goal with NIS 2 is to protect critical infrastructure and organisations within the EU from cyber threats and achieve a high level of common security across the member states.

As such, NIS 2 requires the EU member states to cooperate in the sharing of information to safeguard vital assets from cyberattacks.

Everyone in the "first battalion" from the "Private" to the "Sergeant Major" needs to be aware of what is required of them in order to mitigate risk from the outset.

To manage their information security risks, companies in scope for the NIS 2 Directive must implement an Information Security Management System (ISMS).

"NIS 2 is NIS 1 on steroids"

- European Commissioners, European Cybersecurity Strategy

© 2024 Quantum Evolve Limited

www.quantum-evolve.com

Which supply chain sectors are affected?

Energy (electricity, district heating and cooling, petroleum, natural gas, hydrogen)	Public Administration (central and regional)
Transport (air, rail, water, road)	Space
Banking	Postal & Courier Services
Financial Market Infrastructure	Waste Management
Health (reference laboratories, medical device or pharmaceutical preparation manufacturers and others)	Manufacture, Production & Distribution of Chemicals
Drinking Water & Waste Water	Production, Processing & Distribution of Food
Manufacturing (of medical devices and in vitro diagnostic medical devices; computer, electronic and optical products; electrical equipment; machinery and equipment n.e.c., motor vehicles, trailers and semi-trailers; other transport equipment)	
Digital Infrastructure	Digital Providers
ICT Service Management	Research

© 2024 Quantum Evolve Limited

Minimum NIS 2 requirements:

- Risk analysis and information systems security policies.
- Incident handling.
- Business continuity and crisis management (including backup management and disaster recovery).
- Supply chain security.
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.
- Basic cyber hygiene practices and cybersecurity training.
- Cryptography and (where appropriate) encryption management policies and procedures.
- Human resources security, access control policies and asset management.
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems (where appropriate).

Achieve the requirements by:

- Assessing your readiness.
- Defining your roadmap to compliance.
- Setting up and implementing your risk and security management frameworks, policies and procedures.
- Securing your IT supply chain through supplier due-diligence and remediation planning.
- Optimising your cybersecurity awareness programme.

© 2024 Quantum Evolve Limited

www.quantum-evolve.com

Beware New Regulation

From the 17th January 2025 a new crucial regulation to standardise operational resilience rules within the financial sector is being enforced in EU member states.

The main objective of the Digital Operational Resilience Act (DORA) is to prevent, detect, contain, recover and repair ICT-related incidents, and protect the financial sector during these operational disruptions.

By adhering to the requirements of DORA, financial organisations can proactively manage risks and strengthen their operational resilience.

Regardless of size, all financial entities, and the ICT providers that serve them, are subject to the provisions of DORA and must comply with the regulatory requirements to ensure operational resilience and create a more durable financial system.

But what is the mission manual for DORA
and how do you go to battle?

© 2024 Quantum Evolve Limited

ICT risk management

DORA emphasises the need for a robust risk management framework.

All organisations must take total responsibility for managing digital risks by implementing a governance and control structure. This framework must have a strategy based on risk tolerance that accounts for the recognition, prevention and detection of risk, and demonstrate the ability to respond to disruption, and recover and learn from incidents.

Reporting for major ICT-related incidents

DORA promotes sharing threat intelligence and incident data among financial entities and their third-party ICT service providers to enhance resilience.

DORA requires companies to use a standard methodology for incident reporting and criteria classification to determine the duration, impact and criticality of services affected - significant incidents need to be reported to regulators promptly. This collaborative approach strengthens the sector’s ability to detect, prevent, and respond to operational disruptions.

Management of third-party supply chain risk

DORA highlights the importance of comprehensive supply chain management.

Financial organisations must assess the resilience of their third-party ICT service providers and ensure their compliance with DORA requirements. To help avoid systemic economic disruption, organisations must monitor risk from technology providers throughout the relationship, using appropriate third-party risk management practices.

© 2024 Quantum Evolve Limited

Digital operation risk testing

Organisations should run comprehensive scenario testing of security and resilience. Larger and more influential organisations will require advanced large-scale penetration testing every three years on critical functions and ICT providers performed by an independent tester.

Intelligence sharing for cyber risk / vulnerabilities

The guidelines promote collaboration among financial entities to raise awareness of ICT risks, limit the spread of cybercrime, and support mitigation strategies. By identifying the root causes and lessons learned, organisations can implement proactive measures to prevent similar incidents.

Preparation for the DORA regulation

- Review the relevant legislation to determine if DORA applies to your organisation.
- Ensure the Board is aware of their duties and obligations.
- Conduct a gap analysis to identify areas where your organisation must meet the regulation's criteria for ICT functions, incident collection, reporting, and testing scenarios.
- Develop a plan to address and close any identified gaps.
- Collaborate with stakeholders (such as business continuity, operational resilience, and third-party risk management teams) to prioritise functions and review the results of a business impact analysis or end-to-end mapping.
- Implement the steps before entering an ICT third-party agreement and meet the requirements for exiting contracts.

© 2024 Quantum Evolve Limited

Types of Risk: The Battlefield

Supply chain risk

The supply chain is a vulnerable point in every organisation's defence, often rife with risks.

Picture yourself as a General on the front line responsible for personnel, equipment and supplies. You need all of these to win the battle.

However, your supply routes are being phyiscally targeted by adversaries seeking to disrupt operations, your logistics systems have been subject to cyber-attacks and intelligence activities have gained insights into your military logistics planning.

The successful deployment of military logistics hinges on ensuring that any risks are effectively mitigated against or eliminated in their entirety.

In the same way if your organisation’s supply chain is at risk this will impact the resilience of your business and provide the ability of threat actors to impact your cybersecurity.

“Leaders win through logistics. Vision, sure. Strategy, yes. But when you go to war, you need to have both toilet paper and bullets at the right place at the right time. In other words, you must win through superior logistics.”

- Tom Peters

© 2024 Quantum Evolve Limited

Cybersecurity risk

Cyber-attacks on the supply chain are akin to sneak attacks on your fortress. These include:

Phishing Expeditions

Cyber adversaries send misleading emails to trick personnel into disclosing sensitive information. Remember the Trojan Horse analogy? Well, this is the digital version.

Man-in-the-Middle Infiltration

These cunning foes intercept communication between parties and manipulate data or steal information. It's just like a spy inserted in the middle of your communications network.

Data Espionage

Infiltrators pilfer your precious data, utilising techniques like data exfiltration or eavesdropping.

The risk of exposure or loss resulting from a cyber-attack, data breach or other security incidents is mitigated by performing due diligence before onboarding new vendors as well as ongoing monitoring during the vendor lifecycle.

Legal, regulatory & compliance risk

Your third-parties could impact the measures you have in place to comply with legislation, regulation, or agreements, e.g. the EU's General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS).

© 2024 Quantum Evolve Limited

Reputational risk

No organisation wants negative public opinion.

Some of the most damaging events are third-party data breaches that resulted from poor security controls.

The Trojan Horse springs to mind again.

Operational risk

To stop your logistics disruption to your organisation’s operations, you can contractually bind them to Onboarding requirements including Service Level Agreements (SLAs).

Financial risk

This is the resultant risk that a third-party will negatively impact the financial success of your organisation.

Third-party vendors’ security flaws can facilitate bad actors’ attempts to make their way through your organisation’s secret tunnels straight into your treasure vault.

Strategic risk

Your organisation may fail to meet its business objectives because of a third-party vendor.

All these risks often overlap. For example, if an organisation experiences a cybersecurity breach and customer data is compromised, this could also result in operational, compliance, reputational, and financial risks.

© 2024 Quantum Evolve Limited

Define the Battle

What's the difference between Third-Party Risk Management and Supply Chain Risk Management?

It often comes down to the type of third-party and / or the type of risk you are evaluating.

In order to understand, you need to define the different types of Third-Party Vendor Risk Management.

These include:

Third-Party Risk Management (TPRM)

TPRM is the act of identifying and addressing any type of risk that is associated with third-party entities e.g., financial, fraud, or cyber.

> *"Risk comes from not knowing which cog in your supply chain is in trouble."*
> *- Warren Buffet*

Ⓒ 2024 Quantum Evolve Limited

Third-Party Cyber Risk Management (TPCRM)

TPCRM is a subset of TPRM and is the act of identifying and addressing cybersecurity-related risks that are associated with your third-party entities.

Vendor Risk Management (VRM)

VRM is the act of identifying and addressing any type of risk that is associated with vendor entities.

A vendor is a type of third-party entity that provides a product or service directly to you. All vendors are third-parties, but not all third-parties are vendors.

Supply Chain Risk Management (SCRM)

SCRM is the act of identifying and addressing supply chain-related risks.

There are three types of supply chain attack:

- Compromising commercial software.
- Compromising open source software.
- Embedding malware during the physical production of technology.

© 2024 Quantum Evolve Limited

All Tech Vendors are Vulnerable to Supply Chain Attacks!!

© 2024 Quantum Evolve Limited

Any company that produces software or hardware for other organisations is a potential target for attackers.

Nation-state actors (people or groups who use their technology skills to facilitate hacking, sabotage, theft, misinformation and other operations on behalf of a country) have deep resources and the skills to penetrate even the most security-conscious organisations.

Real-world examples

The SolarWinds Incident

A stealthy invasion, the adversary tampered with the software updates of this networking tools vendor. Once the software was installed, it acted as a spy in the heart of organisations, including government agencies.

Target Corporation's Infamous Breach

Hackers infiltrated the retailer's supply chain via a trusted HVAC (heating, ventilation and air conditioning) vendor. They stole over 110 million customer payment card data records, leading to losses in the millions.

Even security vendors can be targets

In the case of SolarWinds, as many as 250 organisations and 18,000 customers were affected, and the attackers took advantage of multiple supply chain layers.

One of the higher-profile companies breached was FireEye, a cybersecurity vendor.

Other renowned vendors hit by the SolarWinds attackers included Microsoft and Malwarebytes.

© 2024 Quantum Evolve Limited

"Gentlemen, the officer who doesn't know his communications and supply as well as his tactics is totally useless."

- General George S. Patton

Was SolarWinds a third-party or supply chain breach?

The answer is both.

"Third-party" is an umbrella term for all kinds of vendors, suppliers, and partners. So a supply chain vendor like SolarWinds is a third-party, just as a cloud provider or law firm are third-parties.

The SolarWinds breach is also referred to as a supply chain breach because the malware that enabled the breach of SolarWinds customers was embedded in official SolarWinds software updates.

All supply chain attacks are third-party attacks, but not all third-party attacks are supply chain attacks.

© 2024 Quantum Evolve Limited

We Haven’t had Time to Prepare!

These kinds of attacks aren’t a recent development.

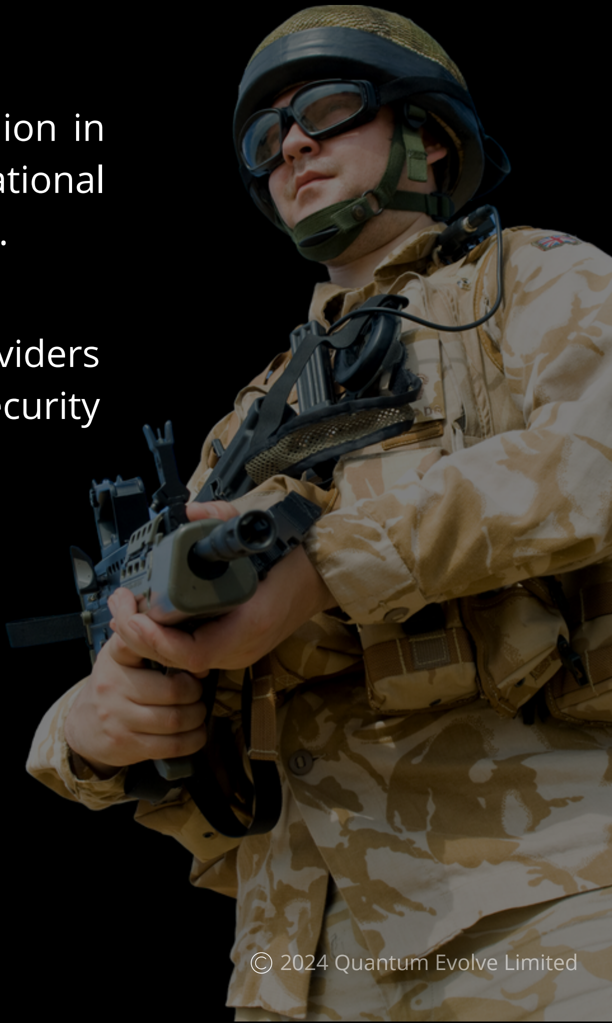
In 2011, RSA Security admitted that its SecurID tokens were hacked. One of its customers, Lockheed Martin, was attacked as a result.

Another supply chain attack in 2017 - attributed to Russia - compromised Ukrainian accounting software as part of an attack designed to target the country’s infrastructure, but the malware spread quickly to other countries.

NotPetya wound up doing more than $10 billion in damage and disrupted operations for multinational corporations such as Maersk, FedEx and Merck.

Unfortunately, many third-party service providers are lax in implementing robust cybersecurity frameworks, controls and strategies.

Therefore, organisations require a Third-Party Risk Management Programme that can assess vendors in the supply chain, communicate threats and respond quickly to security incidents to minimise supply chain risks.



© 2024 Quantum Evolve Limited

Minimise Third-Party Risks

The immediate action you will need to take to mitigate third-party risks depends on the status of your organisation’s TPRM programme.

Firstly, you should assess your current TPRM programme to identify which security measures, if any, you currently have in place. This includes:

Keep an up-to-date vendor inventory

You need to accurately identify who your vendors are. The inventory should be kept up-to-date, track onboarding and offboarding workflows, and extend to fourth parties, namely your third-party vendor’s vendors.

Establish a vendor assessment process

After creating a comprehensive inventory of vendors, you need to develop a third-party risk assessment workflow. Organisations use this process to assess and approve potential third-party vendors and suppliers to ensure they can meet all contracted stipulations and agreements.

> *“If you are going to do TPS, you must do it all the way. You also need to change the way you think. You need to change how you look at things.”*
> *- Taiichi Ohno*

© 2024 Quantum Evolve Limited

"Intelligence is the ability to adapt to change."
- Stephen Hawking

Implement a Third-Party Risk Management Programme

An effective Third-Party Risk Management Programme should consider the following:

- Most organisations manage lots of vendors, with each posing differing risk levels. Each risk tier has a unique due diligence and risk assessment process and other tier-specific requirements, meaning you will need to individually categorise each vendor accordingly.

- Managing a large number of vendors also requires prioritisation of high-risk over lower-risk vendors. However, it is still essential to regularly assess all vendors against the same standardised checks to ensure nothing falls through the cracks.

- For the duration of your relationship with the third-party, you'll need to conduct ongoing monitoring. Some of this will be their responsibility, but you'll also want to pay attention to media reports, business updates, sanctions lists of an international company, breach notifications, and other various methods of gathering intelligence.

This includes maintaining compliance and alignment with all applicable laws, regulations and industry recognised frameworks. Some of the most common being; ISO27001 and 27701, NIST SP 800-53, PCI DSS. There are also more general frameworks, such as the Capability Maturity Model (CMM), ISO 9001, Common Criteria, and SOC 2.

It's your responsibility as an organisation to ensure that you are aware of all regulatory bodies and requirements your company is subject to.

Ⓒ 2024 Quantum Evolve Limited

Let’s Focus on the Cyber Security Risks

It’s estimated that 70% of organisations either have, or are working on, a digital transformation strategy.

Global spending on revolutionising processes, business models, and integrating technology into all aspects of the organisation is expected to reach $6.8 trillion by the end of 2023.

While digital transformation offers enormous upsides for organisations, the digital transformation movement presents a wealth of challenges for cybersecurity teams.

To keep pace, how cyber risk is managed also needs a digital transformation.

Legacy risk prevention practices need an efficiency upgrade. Security teams need to be able to scale quickly to accommodate the influx of third-party tools and cloud-based applications, and security leaders need complete visibility across their entire third-party ecosystem.

Only through a modern approach to Third-Party Cyber Risk Management will security practitioners be able to confidently make data-driven decisions and develop actionable strategies to protect their organisations from threat actors.

© 2024 Quantum Evolve Limited

While an organisation may have strong cybersecurity measures in place and a solid remediation plan, outside parties, such as third-party vendors, may not uphold the same standards.

These third-party relationships can increase vulnerabilities by providing an easier way for potential threats to attack even the most sophisticated of security systems.

Information security teams attend to all other facets of your organisation's security programme and may not have the necessary capability to thoroughly manage third-party risk.

Risk assessments provide deeper insights about a vendor's security posture. When supported by security ratings, this process allows you to track each vendor's cybersecurity levels against industry standards.

Imagine if one of your supplier's suppliers has a ransomware attack that spreads up the chain. An event like this could severely disrupt your ability to do business.

Your security is only as strong as the weakest link in the supply chain.

In the wake of the SolarWinds attack in particular, organisations need to look at their software suppliers, particularly those with software that has privileged access to company assets. That includes expanding assessment criteria to include the integrity of the software development process, and to ensure that controls are sufficient to prevent introduction of malicious code.

"Risk is like fire, if controlled it will help you, if uncontrolled it will rise up and destroy you."
- Theodore Roosevelt

© 2024 Quantum Evolve Limited

The risks associated with a supply chain attack have never been higher, due to new types of attacks, growing public awareness of the threats, and increased oversight from regulators. Meanwhile, attackers have more resources and tools at their disposal than ever before, creating a perfect storm.

The approach will vary depending on each company's available resources, but there are a few points you can consider to address supply chain risks. These include:

- Educating your company's stakeholders about your supply chain process.
- Ensuring you have a reliable method for handling third-party risks.
- Defining your company's third-party risk tolerance.
- Creating a system for continually assessing and monitoring third-party risks.
- Closely tracking people who have access to crucial data in your company.
- Understanding the most vital assets in your company and identifying their location.
- Ensuring that vendor contracts include cybersecurity requirements.
- Periodically testing an incident response plan.

© 2024 Quantum Evolve Limited

www.quantum-evolve.com

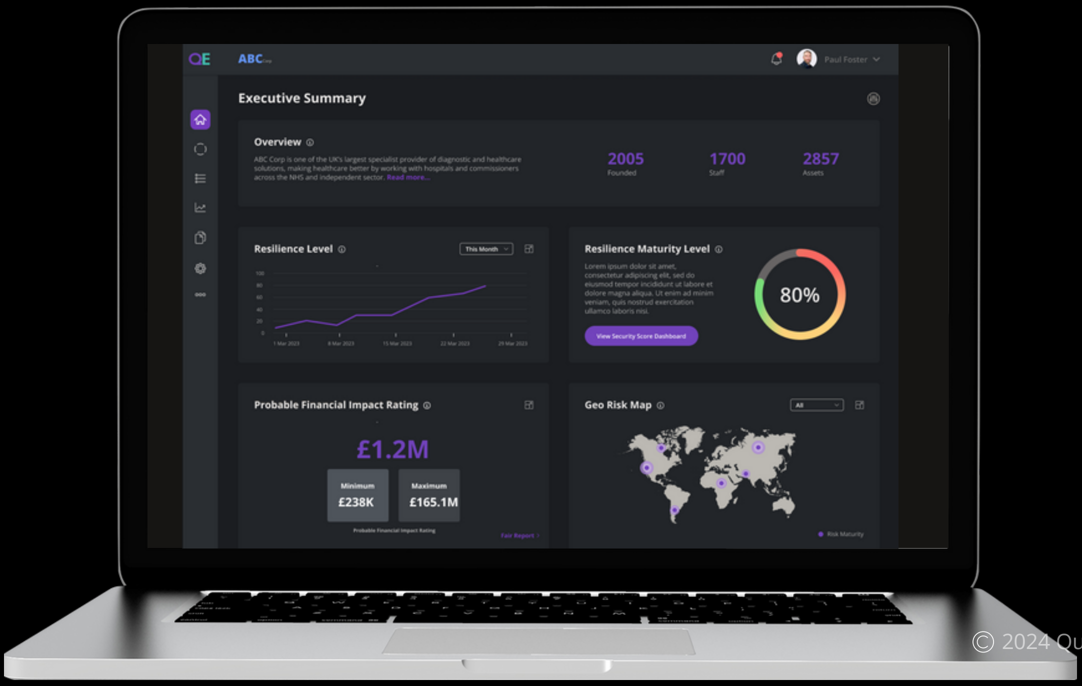
Safeguard your Reputation

Without a clear and complete understanding of your IT estate including your third-party risk, it is not possible to secure a business.

Quantum Evolve's innovative approach to Cyber Resilience & Posture provides your business with a comprehensive understanding of the technical, financial and compliance-related third-party risks within its digital ecosystem.

QE Touchstone, our holistic 360-degree, "single plane of glass" view of your security controls and capabilities, identifies emerging threats, existing vulnerabilities and cyber risks associated with your third-parties.

It quickly and efficiently benchmarks your compliance against globally recognised standards and frameworks e.g. NIST, ISO, GDPR, PCI DSS, HIPAA, NIS 2, DORA thereby safeguarding your network, brand and reputation.



Executive Summary

Overview

ABC Corp is one of the UK's largest specialist provider of diagnostic and healthcare solutions, making healthcare better by working with hospitals and commissioners across the NHS and independent sector. Read more...

2005 Founded

1700 Staff

2857 Assets

Resilience Level

Resilience Maturity Level

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi.

Probable Financial Impact Rating

£1.2M

Minimum £238K

Maximum £165.1M

Geo Risk Map

© 2024 Quantum Evolve Limited

Resilient security posture

We can easily interpret your organisation’s risk from financial quantification to technical detail and analyse your supply chain’s cybersecurity posture.

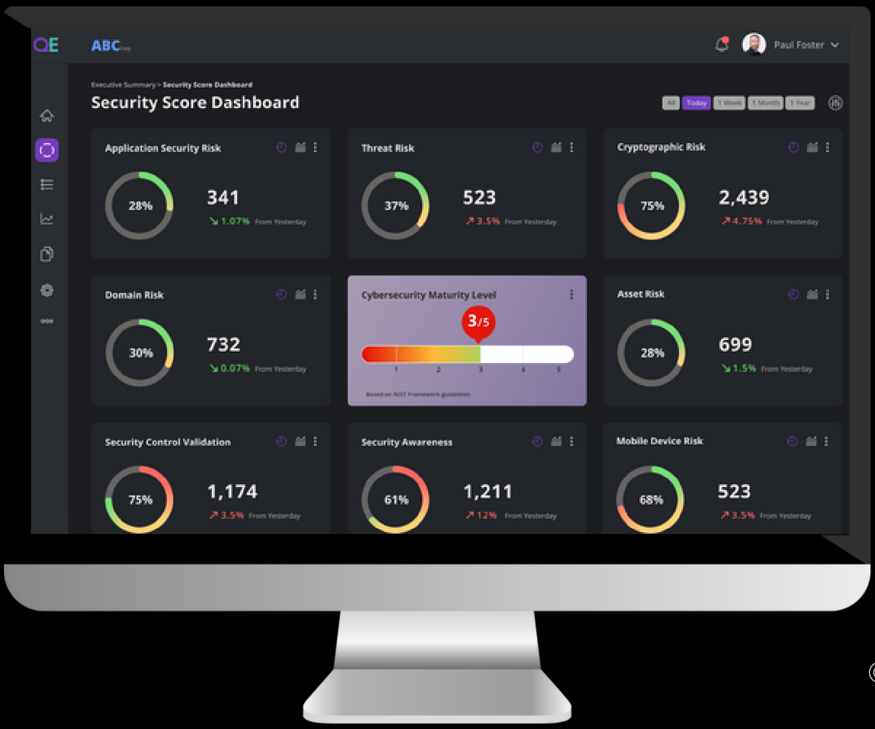
QE Touchstone continuously monitors your third-parties to identify and mitigate ransomware and other risks.

Our Third-Party Risk Management Programme allows us to capture and prioritise your third-party and vendor risks, stating the required remediation, allowing you to develop a clear roadmap to ensure you can modernise, whilst consecutively and effectively mitigating / managing these risks.

Third-party risk assessments

Risk assessments on third-parties ranging from Mobile Device Risk to Cryptographic Risk can be selected from QE Touchstone’s wide-ranging services and tailored to meet exact requirements.

Should you wish to find out more information on the solutions and services Quantum Evolve can provide, please contact one of our experts.



© 2024 Quantum Evolve Limited

QUANTUM
EVOLVE
Business & Cybersecurity Resilience Consultancy

QE Touchstone
Assess, Protect & Continuously Monitor

Michael (Mo) Stevens, Chairperson
+44 (0)7801 712582
michael.stevens@quantum-evolve.com
michael-mo-stevens-b42b61

Mark Child, CEO
+44 (0)7515 107005
mark.child@quantum-evolve.com
mark-child-8859451

Paul Foster, CTO
+44 (0)7450 872368
paul.foster@quantum-evolve.com
paulfosterconsultancy

www.quantum-evolve.com
quantum-evolve-business-enablement

CYBER ESSENTIALS CERTIFIED PLUS

MSDUK CERTIFIED ETHNIC MINORITY BUSINESS

© 2024 Quantum Evolve Limited