

Delivering Complex Technology Capabilities

"The project was off-track, late and costs were rocketing. We thought we were alone and that no-one could provide technical, financial and management support that we needed. We were wrong. In six months, CyberVector turned the project around. We were made into a better team, with new insights and abilities. We delivered successfully."

Just one case where we made the difference.

We can make the difference for you too.

About CyberVector Ltd

In one form or another we have been in business for over 20 years. All of our delivery staff are positively vetted and security cleared.

We have backgrounds in software, hardware, science, engineering, information science as well as project, programme and risk management.

Many of our people have worked in embedded high performance teams, often badged as our clients. We blend in. We believe in setting positive examples and display attitudes and behaviours that are underpinned by our culture.

When we work for you, no one will ever know.

"We needed experts to help us procure high technology solutions for problems we anticipated 5 years into the future. CyberVector staff seamlessly blended into our teams, working with the same conviction and purpose as our own employees. They brought expertise and tools that we simply didn't have, and were instrumental in enabling us to be ready for the emerging challenges. We couldn't have done it without them

— Non-Executive Director, HMG Government Agency



CyberVector specialises in the delivery and support of data, information and intelligence rich projects and programmes.

We work with UK FTSE100 private sector companies, and departments and agencies of Her Majesty's Government.

We are a privately owned UK company with no non-UK shareholders, controlling interests or oversight.

For more information visit CyberVector.co.uk

Troubleshooting Failing Projects And Programmes

The Problem

At any time you have a number of projects underway. Too often small errors become compounded and, initially, go un-noticed or are ignored. Eventually issues mount up, problems occur and, suddenly, the project is failing.

Significantly, this has consequences on other projects across the portfolio, to programmes and to your organisation.

You have to put this right.

We have over 20 years of experience in troubleshooting failing projects and programmes. We have a proven systematic approach to diagnosing the causes of failure, establishing methods of recovery and turning projects around. Our tools integrate with your project, programme and portfolio management applications to provide accurate, detailed data and information that form the basis of the project recovery.

We can often identify and implement quick rescue actions within two days, and we increasingly get called on for project initiation, getting your activities off to a sound and successful start.

We work alongside your staff or your chosen project management consultants or providers. We help them to learn how to avoid making similar mistakes again, improving their performance and encouraging best practices that they can use repeatedly and with confidence.

"CyberVector fielded a security cleared, multi-disciplinary team that motivated the down-beat in-house project staff and quickly established the root causes of our difficulties. They adjusted the deployment, created a rescue plan and worked with us to successfully turn the project around"

— Director, Missile Programme, Global Defence Company.

Operational Intelligence — Fact Based Decision Making

The Problem

You have a lot of data and the technology to support it. You hope that your decisions are based on facts.

But, do you know what data really contributes to your organisational decision making? Do you know how well supported your decisions are? Does your data reflect changes that affect your business? Can you respond with agility and confidence?

Probably not. And you're not alone.

We help you to really understand your how to make decisions using the data, information and intelligence you have. We refer to this as your Decision Architecture.

We see data and information as historic to your organisation. Important but not, in themselves, the real source of decision making. We'll run organisations make decisions about the future state and how to reach a particular destination through informed action.

Decision Architecture quantifies how data creates information, how information creates intelligence, and how intelligence supports actions and decision making.

We work at pace, using our proprietary tools, to help you get the most of your data and make the right operational decisions.

"We had so much data, and yet we couldn't see what was important. We had experts that came to conclusions that were different from other experts using different data segments. CyberVector helped us simplify the data estate, enabling us to extract consistent information that made a tangible difference to the success of our business and operations"

— CEO, FTSE 100 Retailer

Data Grenade — Protect ALL your data from ransomware

The Problem

Zero Day viruses and ransomware sit dormant in your system, waiting for the right trigger to activate. It doesn't attack your operating system, but finds your data and renders it inaccessible.

Data Grenade fragments all of your data, rendering all viruses and ransomware inactive. It's like taking a biological virus and splitting it into separate DNA chunks. Only the reassembly of the separate chunks, in the right order restores the original object; in time for a cure.

Data Grenade works for datacentres to personal users.

In 2020 the basis for Data Grenade was successfully patented. The approach efficiently fragments any type of digital object (whether pictures, documents, executable code, anything) into a random number of pieces of random size. Only the Data Grenade application knows which pieces of data, stored in common cheap storage, belong to a particular item of source data, and in which order they need to be reassembled in order to recover the original item.

Source objects of any security classification, from as low as OFFICIAL to as high as TOP SECRET, can be protected, with the file fragments able to be stored in unclassified cloud storage, or on-premise, or in hybrid systems.

The Data Grenade uses high degrees of mathematical complexity instead of encryption key-pairs. No need for key exchange or management. No cumbersome initial exchange weaknesses. Data Grenade protects everything and cannot be brute force attacked.

"We have a real concern about ransomware. We want to protect all of our clients' data and Data Grenade is a cheap, comprehensive and easy to use means of achieving that." — Head of Cyber Security, UK Sovereign Datacentre Business

Data and Sensor Fusion

The Problem

Your data comes from a wide variety of sources. The temporal, spatial, spectral and sampling rates are different. You can't just overlay the data to give you an accurate representation of the current or future states.

This isn't uncommon, but getting it right isn't trivial. Getting it wrong is easy and will really have a negative impact on your business and operations.

You're not alone. We address these problems all the time and have done for years.

Data tends to have different spatial, spectral, temporal and sampling resolutions. Data can be structured or unstructured. Combining data is fraught with difficulty.

We've been developing algorithms to address these issues for over 20 years. Whether you're combining radar, infra-red and spatial data or triangulated radio transmissions in a rich urban context, we can help you fuse your data correctly.

Post processing data, even in real-time, for a data fused picture is very different from fusing data on the fly at the platform sensor level. We work with sensor producers and platform integration prime contractors to enable them to combine different types of sensor data to improve discrimination and accuracy. We do this at the hardware level, at the sensor operational rates.

"We tried to enrich our knowledge by combining various data types, but we really couldn't see the wood for the trees. After three weeks working together we had completely transformed our understanding, and could use our data to make powerful conclusions." — Head of Development, Remote Sensing Company

Technology Re-platforming — Improve Performance And Resilience

The Problem

Over the years you have developed software to standards, but these were not rigorously enforced and not thoroughly checked.

Developers and standards have changed and now your applications are running on legacy hardware and obsolete systems.

These applications are important to you, so out-of-date systems and technology are maintained because you can't be sure that you can migrate onto new computing surfaces. Your costs are high and, some time, something will fail.

We have worked with CRAY, Thinking Machines, Silicon Graphics and many other linear, vector and parallel architectures, and written in Pascal, COBOL, FORTRAN, all flavours of C and Java. We have written at the directive and assembly levels. We have experience of all major operating systems.

We understand software development from the functional, logical and encoding levels. And we have developed complete testing and quality assurance reviews.

We can rewrite your code to rigorously enforced standards. We can undertake anything from a like-for-like conversion, to a full redesign from a functional perspective onwards.

We can develop highly performing algorithms that make the most of current memory and processor architectures to complete the operations that are important to you in better, more efficient ways than legacy algorithms.

"The costs of maintaining legacy software and obsolete systems were rapidly increasing. CyberVector planned and undertook a phased re-platforming with a flawless switch-over." — CIO, FTSE 100 Financial Service Company

Cyber and Information Security — Defend Through Knowledge Of Attack

The Problem

You have a well defined secure perimeter, but your business has expanded and you have more sub-contractors in your supply chain that have connections into your data estate. Your direct internet controls and connections are well protected, but you have been compromised somehow.

You need to establish how this has happened and prevent future occurrences. You do not know how to ensure that your sub-contractors are not the weak links through which you are being hacked.

Cyber is used to mean a lot of things. We take it to mean the totality of some more fundamental components, these being Information Security and Information Assurance, Risk Management and Threat Specific Measures.

Our approach is to fully understand each component in its own right, and then understand how these come together to create something greater. In each case our mathematicians, information scientists, protocol and system specialists, code developers and threat-vector designers begin by thinking like the threat-actor. By taking the "red" rather than the "blue" perspective we develop an attack design, which we call the Anatomy of Attack. Through the use of highly representative test environments, we assess the impact of any particular attack, looking for tell-tale measures that characterise its effects.

With a characterisation, we then develop the triggers and counter-measures to effectively combat the particular attack. This may result in new technologies, policies and processes, or training and situational awareness.