daisy.

CYBER SECURITY REVIEW

SENIOR EXECUTIVE REVIEW

Including Ransomware
Preparedness Assessment

DAISY SERVICES

We have now all seen how a cyber security breach can cripple IT systems, and destroy organisational and individual management reputations. Therefore, it is important that senior management understand how well they are protected. Due to the technical nature of cyber security, all too often business leaders feel in the dark about whether their protection is effective or not.

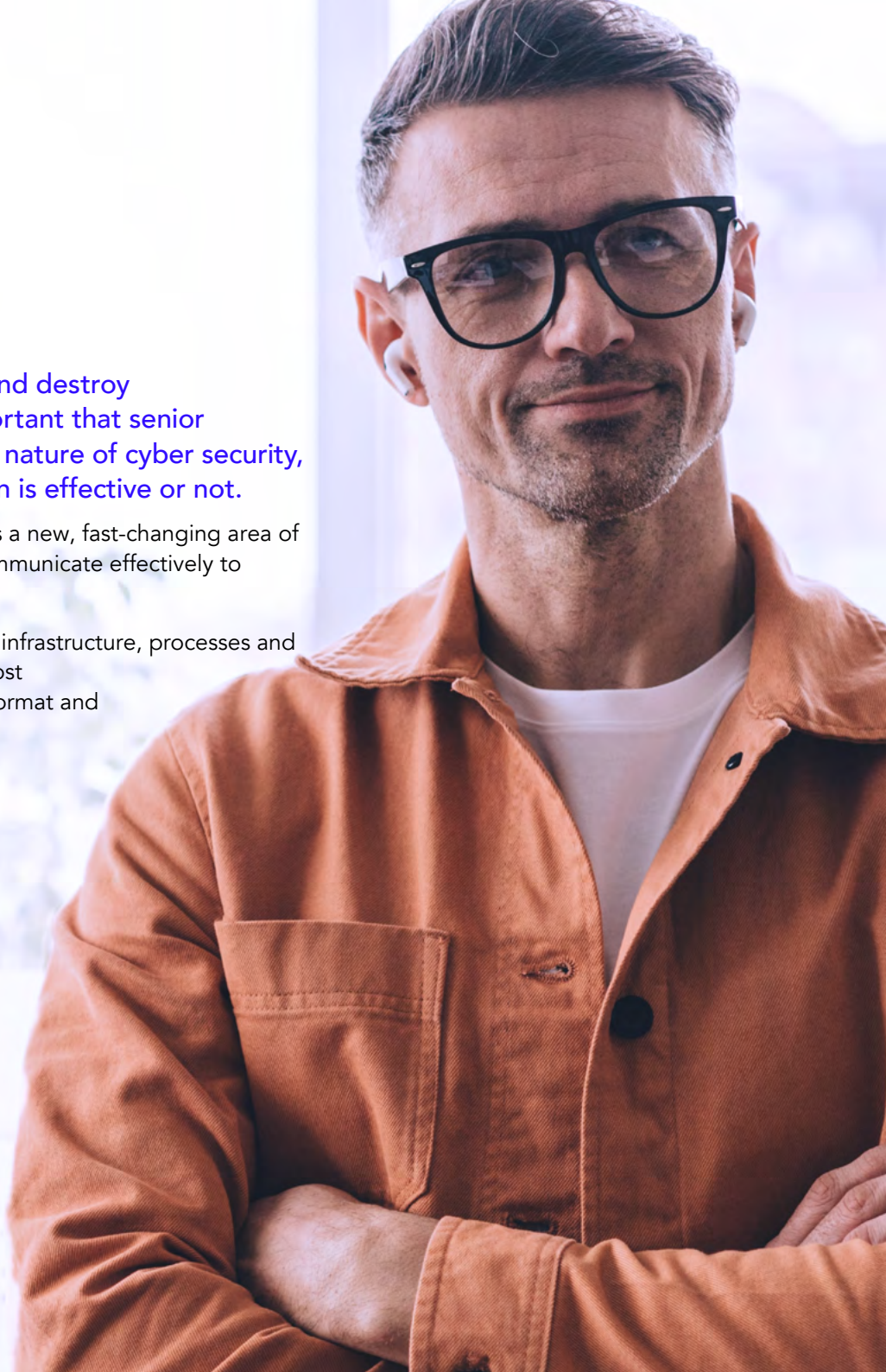
Cyber security presents many challenges to board-level executives and business heads. It is a new, fast-changing area of organisational risk, with few people that understand it: of these people, even fewer can communicate effectively to senior management.

Our Cyber Security Review is designed to assess the key aspects of your IT security-related infrastructure, processes and technical management capabilities, and balance these against the cyber threats that are most relevant to your business. Most importantly, our Cyber Security Review outputs these in a format and language that is designed for senior (non-IT) managers and organisational executives.

In addition, the unique reporting methodology allows you to target future improvements and measure your progress towards this goal. It allows you to see when you have an appropriate balance between risk and protection - a pragmatic approach that gives clear justification for any investments in this area.

Our Cyber Security Review can also map your current compliance to the Information Commissioner's Office (ICO) GDPR security outcomes, should you opt to. These are now regarded as the appropriate framework to prevent a personal data compromise.

> ***"What impressed the management team was your ability to translate very technical issues into language understandable by non-experts and explain the associated risks."***
>
> **CTO, Financial Trading Systems**



UNDERSTAND YOUR RISKS

Our aim is to help you understand your current situation, and help you execute pragmatic improvements that directly relate to your current risk of a serious cyber security breach.

The four components of our Cyber Security Review include:

1. Cyber Security Priorities
This covers the areas of IT security protection that directly impact on your risk of a serious cyber security breach, and the ICO expected security outcomes.

Whilst our expert analysis is in-depth, we report these as either red/amber/green, accompanied with specific recommended and targeted improvements, where necessary.

2. Cyber Security Matrix
Our unique scoring tool is designed to give you an overview of your current level of protection and the risks your organisation faces.

As your protection should be commensurate with your risks, we don't just compare you with some hypothetical ideal. Rather, we look at the balance of your risks, in the context of the nature of your operations, and your current capabilities and weaknesses.

3. Cyber Security Quadrant: (Organisational Risk)

This is an executive-level reporting system that gives management a clear picture of your current security position and facilitates resource decisions.

4. Cyber Security Quadrant: (Ransomware Preparedness)

This is also a useful executive-level reporting system that evaluates your organisation's ability to quickly and effectively respond to a ransomware attack.

By reporting in a language and format familiar to management, we can facilitate critical discussions and decision-making regarding critical improvements.

CYBER SECURITY PRIORITIES

Not everything that information security professionals spend time on has a significant impact on preventing breaches. For example, in many incident responses we find that the local security personnel have done extensive work on impressive documentation, whilst significant technical vulnerabilities have been ignored.

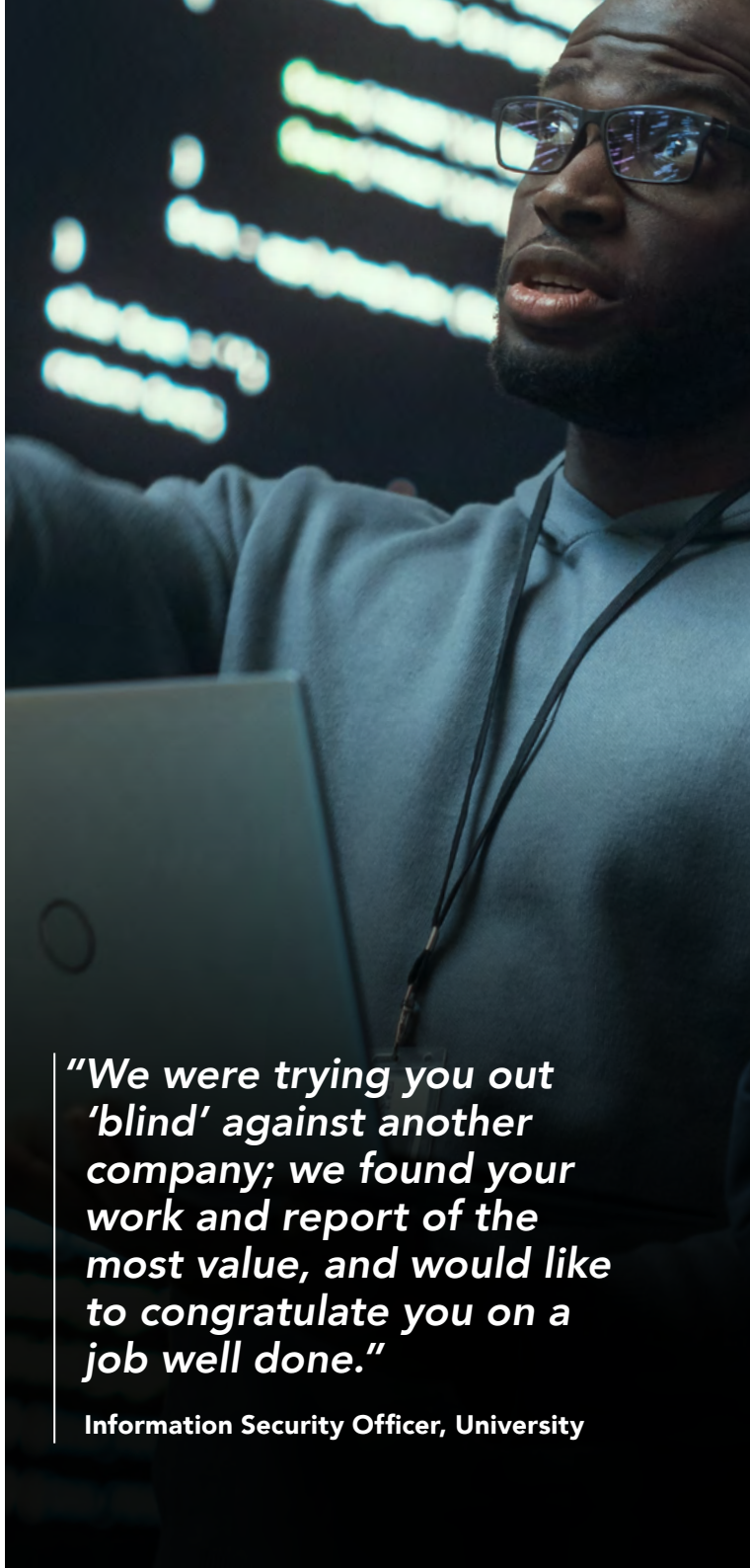
So, we have combined over two decades' experience of incident response, and the associated root-cause analysis, to develop a set of cyber security priorities. These are the most fundamental countermeasures that, if not properly deployed, tend to lead to security breaches. In general, cyber security breaches tend to originate through two attack vectors:

1. IT systems visible to the Internet, that are subject to constant probing for vulnerabilities.
2. Users, either exploiting technical vulnerabilities or tricking users into actions that help the attacker.

We utilise different sets of priorities for these two main categories, ensuring both routes are appropriately assessed, and subsequently protected.

Critically, we don't just look for evidence that you have these technologies in place. Rather, we carry out a detailed examination of configuration and management processes to determine how effective each technology is in preventing a breach.

Whilst our expert analysis is in-depth, our reporting is simple, with either red/amber/green, accompanied with specific recommended and targeted improvements, where necessary. This is essential to get your local team, or external support, working on the areas that have the biggest impact in breach prevention.



"We were trying you out 'blind' against another company; we found your work and report of the most value, and would like to congratulate you on a job well done."

Information Security Officer, University

CYBER SECURITY MATRIX

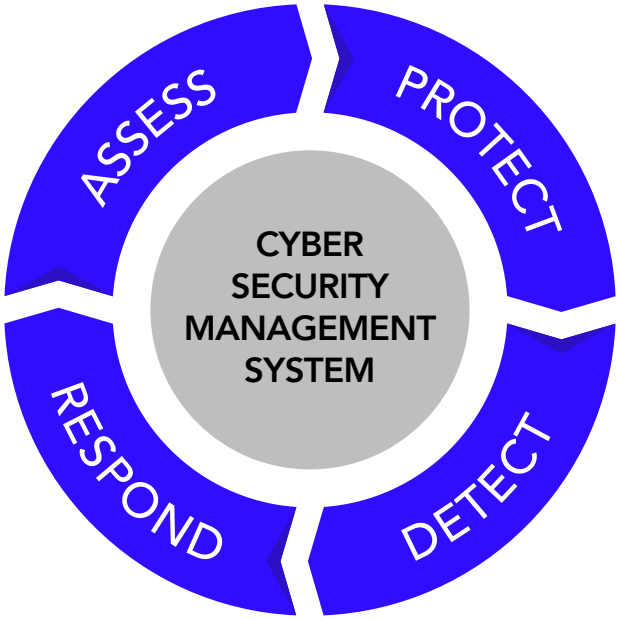
Building upon our expertise in breach root-cause analysis, and the associated technical priorities, we then broaden our review to look at wider aspects of security management that directly impact on breach prevention. We group these into the following areas:

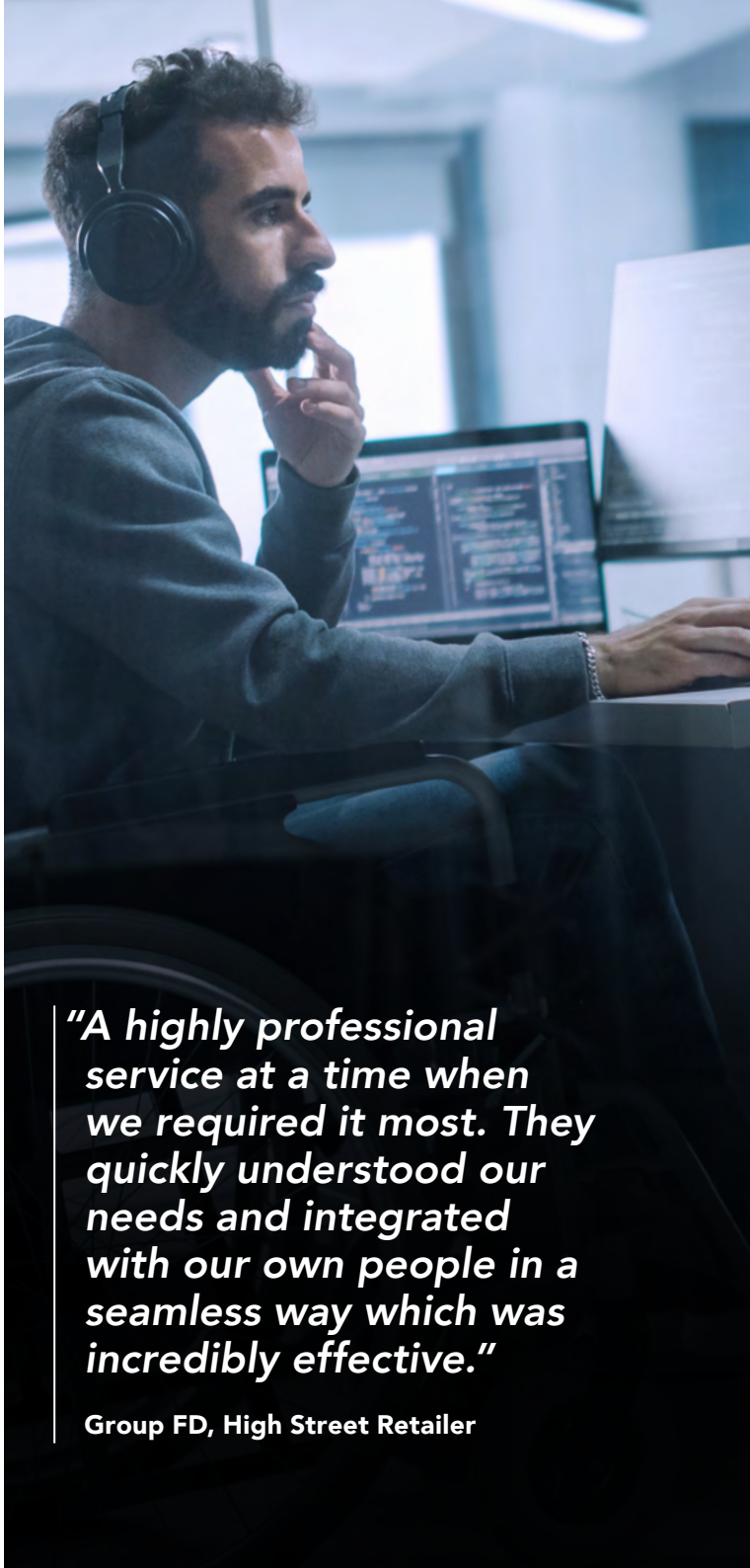
- Security technologies
- Vulnerability management
- Systems configuration
- Systems monitoring
- Team expertise

The relevant importance and weighting given to the outputs will be guided by a review of your risk position, which will assess the following:

- Systems visibility
- Target information and/or systems
- Customer interest
- Regulatory/legal compliance
- Third-party risks

This process gives you an essential assessment, as part of our security management system model:





"A highly professional service at a time when we required it most. They quickly understood our needs and integrated with our own people in a seamless way which was incredibly effective."

Group FD, High Street Retailer

CYBER SECURITY QUADRANT

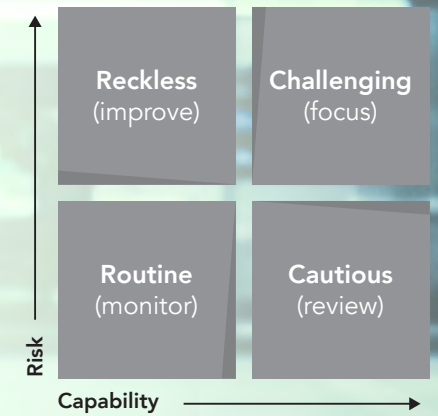
INC. RANSOMWARE PREPAREDNESS

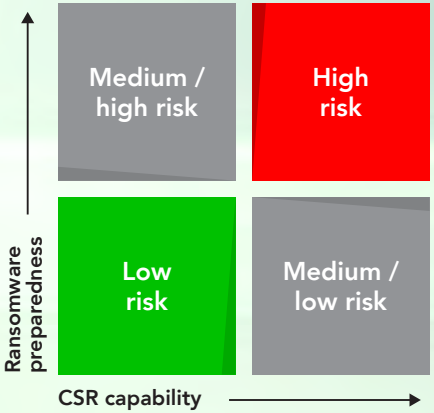
An essential element of our Cyber Security Review is to translate potentially complex technical information into the language that management will understand.

We develop a scoring based on our cyber security matrix, and express this in a familiar format. This mirrors many existing senior management approaches that help executives understand relatively complex areas of organisational management.

This tool, unique to us, facilitates:

- Evaluation of your current position, this includes an evaluation of your ability to respond to ransomware attacks
- Understanding differing positions across the organisation
- Identifying areas of under (and over) spending on security
- Benchmarking and measuring future progress





daisy.

NEXT STEPS

If you want to find out how Daisy can help you to improve your cyber security, contact us on:

0344 863 3000

Or if you're an existing customer, get in touch with your account manager directly.

daisyuk.tech