daisy.

MANAGED DETECTION & RESPONSE (MDR):

An essential guide to the fundamentals of cyber security for Chief Financial Officers

Cyber Security

WHY CYBER IS IMPORTANT TO YOU

Cyber security is now firmly on the board agenda. Effective cyber security can reduce risks to your critical data, reputation, operational systems, and profitability. However, you must do more than simply place all your trust in your IT team as the proverbial buck for accountability does not stop with them.

It is important for CFOs to understand exactly what their current cyber security provision delivers and what it doesn't. and how this fits in with the organisation's approach to risk management.

This guide is intended to be an introductory document to help finance directors, and your executives, understand the importance of monitoring critical cyber vulnerabilities, detecting ongoing breaches, and containing them before they escalate into major breaches.

There is now a real understanding that cyber security breaches can, and do, affect organisations of all sizes and across all sectors. Your IT department is likely to be struggling to keep up with the latest threats, impacted further by the challenges of recruitment and retention of cyber security specialists.

In our experience, damaging security breaches can be avoided with a pragmatic approach in the identification of relevant risks, and subsequent actions to minimise the amount of damage that can occur to your IT systems and critical data.

The most significant ROI for any cyber protection solution is to identify incidents early, and allow containment before an attack becomes a loss of confidential personal information or ransomware, leading to business down-time, significant fines, and reputational damage.

You are living through a period of ever increasing focus on cyber security from your:

- **Regulators**
- **Customers**
- **Employees**
- **Third-party stakeholders**

ARE YOU A TARGET?

Some people have fallen into the dangerous trap of thinking, "Are we a target?", and deciding an answer such as, "No, we are not a bank".

Unfortunately, the reality is that everyone is now a target. Often, just ignoring your cyber security responsibilities is enough to attract the attention from hackers. For example, any system attached to the Internet will be scanned many times each day by hackers looking for these easy 'targets'.

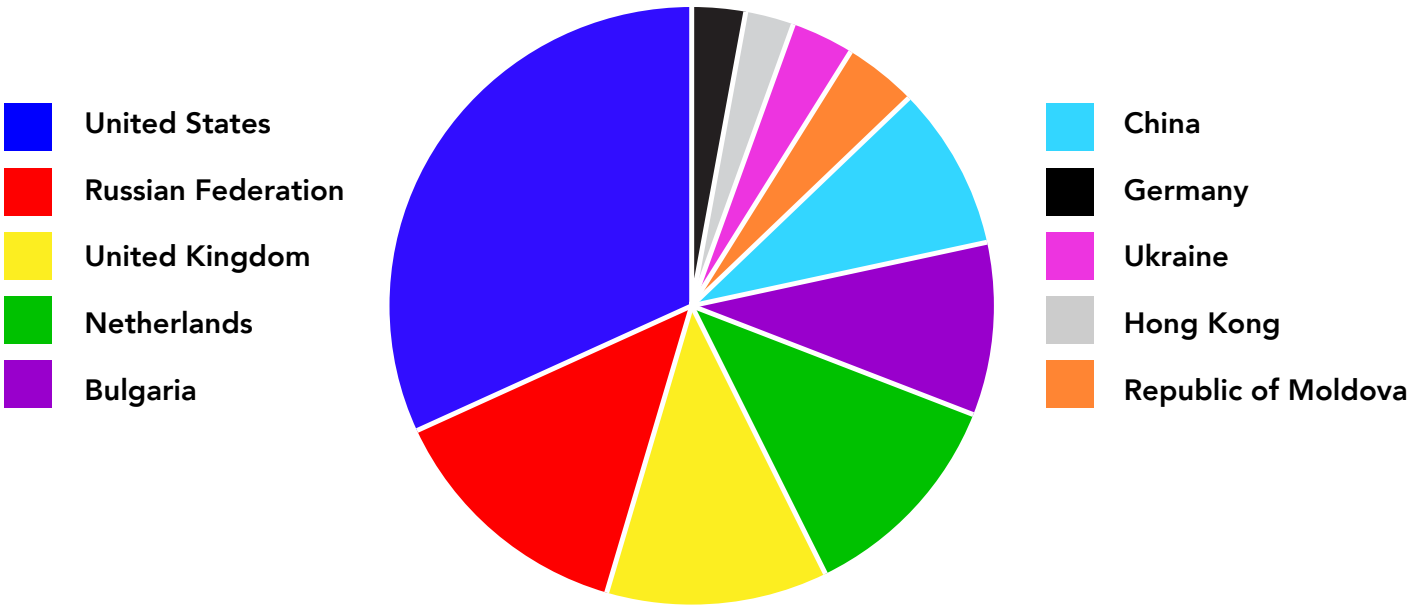
Let's look at what this means for a typical organisation. Below is an example illustration of 'attacks' directed at one Daisy customer in a single day. You can see the countries where attacks originated.

The first interesting fact is that the total number of attacks is more than **200,000 in a single day**. Secondly, note that the hackers are using many 'trusted' countries to launch their attacks.

So, which interesting target organisation is this customer example from? You may be surprised to learn that this is a relatively small Housing Association. Not where an organisation might expect hackers to 'target'.

Hackers are looking for weaknesses in all organisations continually all day, every day, not pre-selecting based on size or sector.

Attacks Directed at a Daisy customer in a Single Day



CYBER SPECIALISTS ON YOUR SIDE

You will see regularly in the press that details continue to emerge of serious breaches and the significant consequences for organisations unlucky enough to be victims.

Of course, these are only the tip of the iceberg, with most breaches not making the headlines, and the majority remaining either unreported or even undetected.

It is now clear that you need the latest specialist skills, knowledge, and experience on your side if you are to counter this ever-increasing threat to your systems and information.

With the expertise required to protect you in short supply, it makes sense to leverage the expertise of a trusted partner such as Daisy.

With the introduction of GDPR, the National Cyber Security Centre (NCSC), as part of GCHQ, identified two significant benefits from professional detection and response services:

- **Detecting attacks as they happen**
- **Helping you to recover quickly from a cyber incident**

Successful detection and remediation of attacks reduces the risk of severe systems disruption, removes the need for any ICO (and other regulator) reporting and avoids GDPR fines of up to 10 million Euros, or 2% of turnover (whichever is higher).

CAN YOU TRUST YOUR IT TEAM?

Yes.

You can usually trust them to do their best, with the resources you give them, to deliver new IT projects at the same time as maintaining (sometimes legacy) systems.

However, can they do this at the same time as monitoring, and understanding, new cyber security threats and vulnerabilities without a dedicated team?

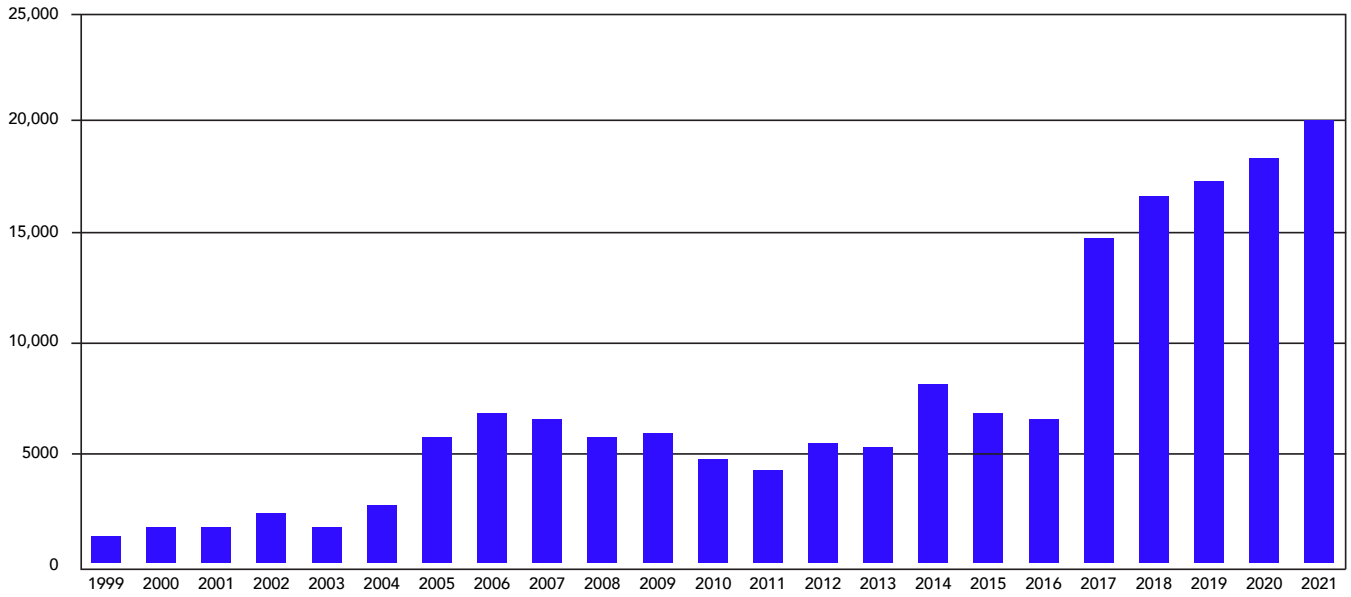
The graph below shows the increasing rate of new cyber vulnerabilities discovered in IT systems.

You will see that in the last 5 years, this has grown to more than 20,000 per year. That is an average of 55 per day!

So, unfortunately unless you have the resources to build a significant internal team of cyber specialists, you will need external support to understand this ever changing risk environment.

In addition, hackers don't work business hours. Therefore, your monitoring, detection, and response to new threats and breaches needs to be 24/7/365.

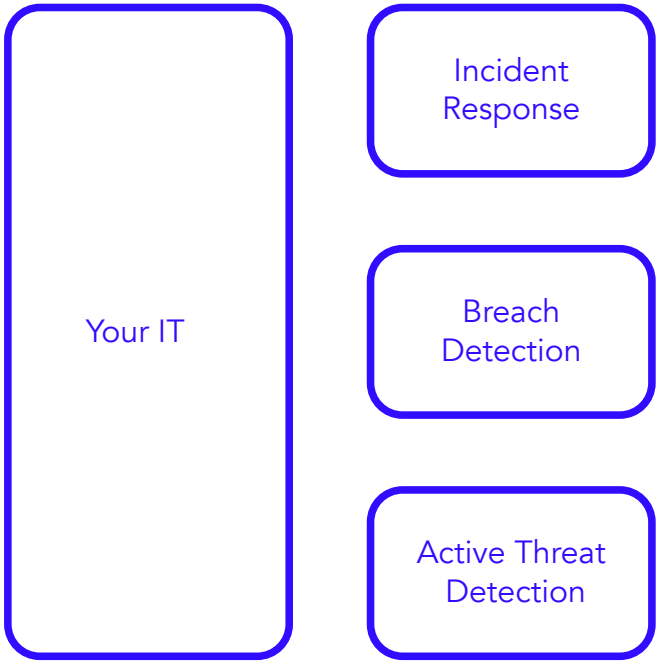
The Increasing Rate of New Cyber Vulnerabilities Discovered in IT Systems



So, what does Daisy provide to CFOs to address these risks and challenges?

MANAGED DETECTION & RESPONSE

Given that your IT team is unlikely to have the necessary expertise, or staffing to monitor 24/7, Daisy has developed three critical cyber security managed services to sit alongside your IT people, processes, and technologies, reporting directly to yourself.



Incident Response

If the worst happens, our experienced incident response team are on-hand to guide you, either remotely or on-site. This response includes not only the necessary technical response, but also guidance to management on all aspects of crisis management.

Breach Detection

Using our 24/7/365 Security Operations Centres in the UK and Australia, we monitor your IT systems for the first signs of a 'successful' breach, giving you early warning and time to respond before a breach escalates into data-loss or ransomware.

Active Threat Detection

Overnight scanning and testing of your systems identifies misconfigurations and mistakes that are potentially risky, before the hackers spot this and start to target you. Then, knowing what services you are using that are Internet-facing, we give you the latest information on new vulnerabilities every 8 hours, seven days a week.

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