GALLAGHER Security

How to recognise a cyber-responsible vendor in a business integrated world

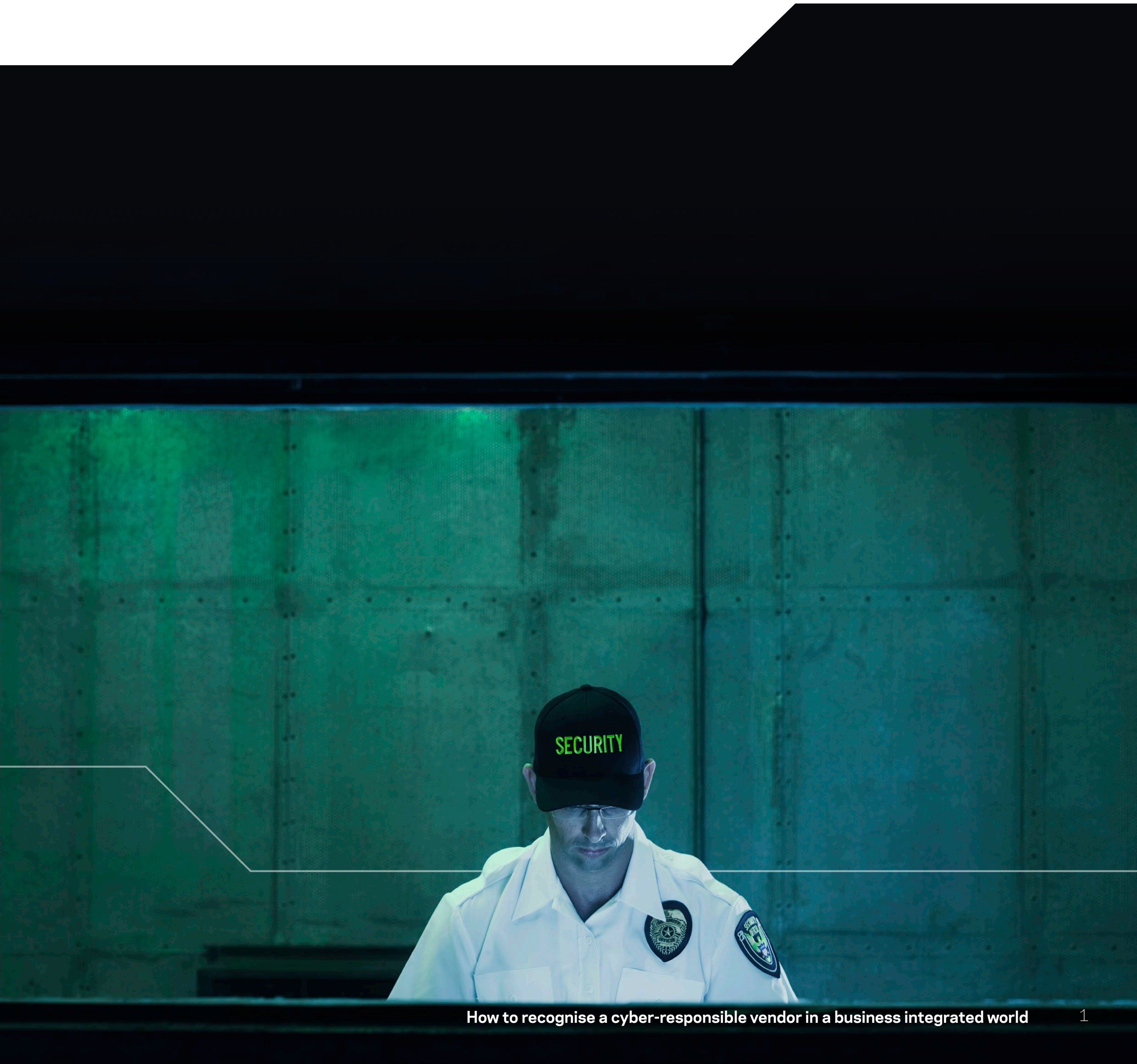
In a world where cyber threats are evolving and ever-changing, are we prepared for an attempted attack? What is the risk to our organisations, and are our security systems up to the task of protecting against unauthorised access to our data?

We're going to look at the relationship between cyber and high security, define what cyber security is and why it is so important, detail how to recognise a responsible cyber vendor, and discuss why organisations of all sizes should consider government-approved security solutions as part of their cyber protection.

What do we mean by high security?

High security refers to the protective security measures put in place by governments to protect data and assets. Government standards and the compliance to those standards are some of the most challenging for a security product vendor to achieve.

As the world becomes more technology driven, high security solutions are finding a place in the commercial world, offering high-quality protection which reduces the risk of cyber-attack. A visibly strong security system acts as a deterrent to hackers – who typically favour weaker technology which is easier to penetrate and presents a lesser chance of getting caught in the process.



What is cyber security and why is it important?

Cyber security is how organisations reduce the risk of unauthorised access to information. It's the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks.

With smartphones, computers, and the internet such a fundamental part of modern life, cyber security has never been more important.

Cyber breaches pose a real threat and the effects can impact everyone. There have been several well-documented examples of cyber breaches over the years – for example, the 2015 hacking of a Ukraine energy distribution company[1] which saw electricity supply temporarily disrupted for more than 230,000 people after 30 substations were taken offline.

The WannaCry Ransomware attack is another example where it is estimated more than 200,000 computers across 150 countries were targeted, encrypting data and demanding ransom payments in Bitcoin cryptocurrency[2].

Cyber breaches can be both inconvenient and costly for targeted individuals and organisations. According to the IBM *2020 Cost of a Data Breach Report*, data breaches cost UK enterprises an average of £3 million (US$3.9m)[3] per breach and it took an average of 256 days to identify and contain the breach. Fifty-two per cent of data breaches were caused by malicious attack – the majority of which were caused by compromised credentials, cloud misconfiguration, or a vulnerability in third party software.

Thirty-three per cent of UK organisations say they lost customers after a data breach and 44 per cent of UK customers claim they will temporarily stop spending with a business after a security breach. Forty-one per cent claim they will never return to a business post-breach.

As technology advances, so too does our interconnectivity between devices, networks, and systems. Each new thing connected to your platform or network is a potential vulnerability – your system is only as strong as the weakest device. It's imperative the technology and risk correlate.

Is this relevant to me?

It can be easy to dismiss the risk of cyber threats. Our perception of these threats leads us to assume we understand a hacker's motive and know what organisations they are interested in, what data they're looking for, and what they're planning to do with the data if their attack is successful. In reality, this information is difficult to predict. The misconception that hackers only target large organisations or critical sites can lead to complacency when it comes to cyber security, with people thinking 'that won't happen to me'.

Unfortunately, cyber threats are a very real threat to all organisations, regardless of size or industry. In the United Kingdom, a small business is successfully hacked every 19 seconds – up to 88 per cent of companies suffered breaches in the last year. Around 65,000 attempts to hack small-to-medium businesses occur in the UK every day – 4,500 of which are successful[4]. Ransomware attacks are on the rise and threats are evolving rapidly.

Corporate Vice President of Microsoft, Tom Burt, said, "The escalating attacks we've seen in recent years are not just about computers attacking computers – these attacks threaten and often harm the lives and livelihoods of real people, including their ability to access basic services like health care, banking, and electricity"[5].

Microsoft's recent Digital Defense Report[6], which covers cyber security trends from the past year, makes it clear that threat actors have rapidly increased in sophistication. The report identifies clear preferences threat actors are showing for certain techniques, with notable shifts towards credential harvesting and Ransomware, as well as an increasing focus on Internet of Things (IoT) devices. The first half of 2020 saw an approximate 35% increase in total attack volume compared to the second half of 2019.

With the events of 2020 fuelling the working from home movement, many employees are connecting to work via home or private networks, making organisational security policies harder to enforce and increasing the risk of cyber breaches.

As we've established, high security solutions can offer effective protection against these escalating attacks. These solutions are not restricted only to organisations operating within the high security space; they are available commercially for any organisation seeking a strong, robust solution that adheres to national standards.

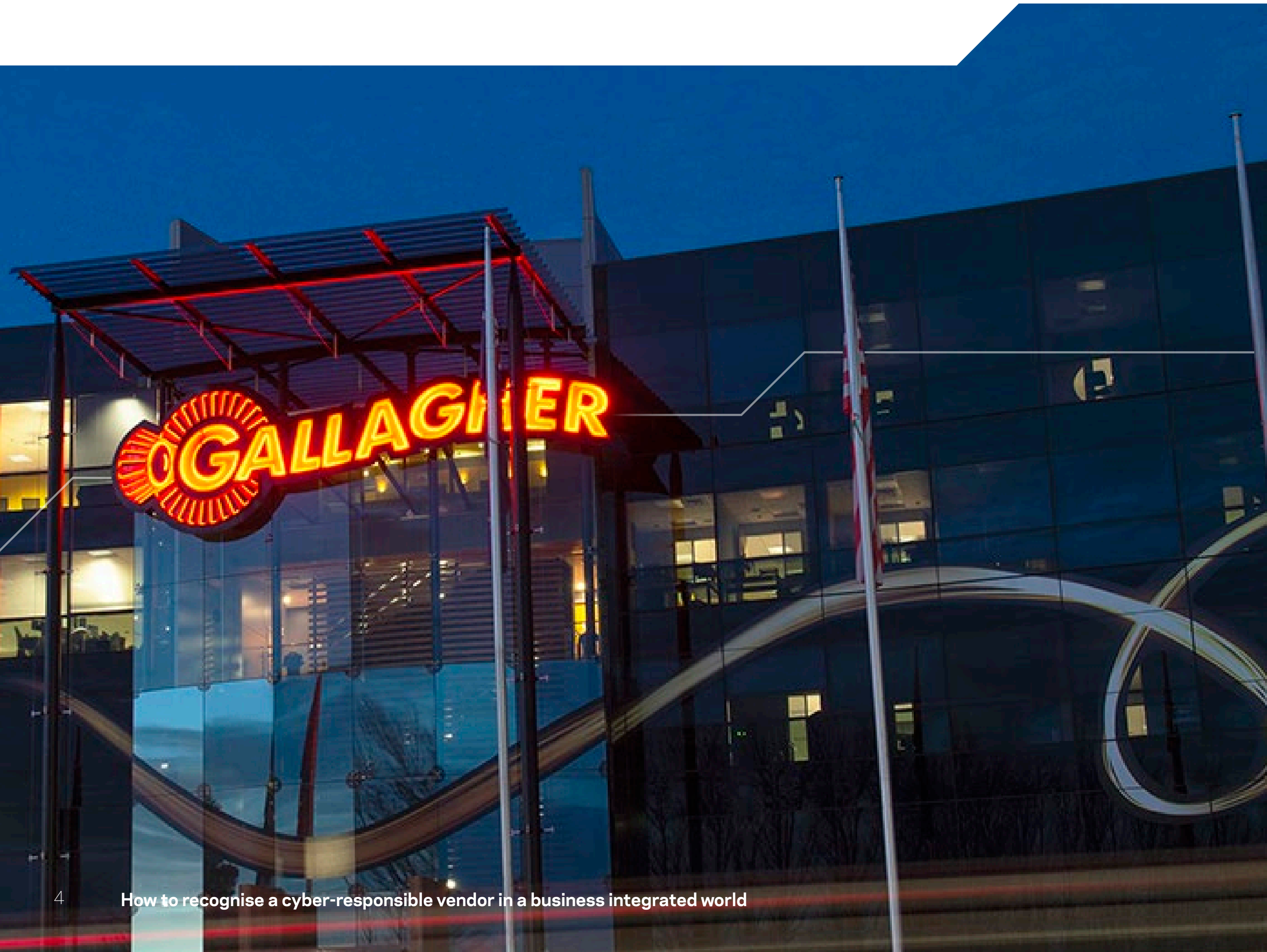
How to recognise a responsible cyber vendor

There are several things to look for in a manufacturer of cyber and high security solutions. It's not enough that products are aesthetically pleasing and intuitive to use, products should be assessed for in-built defensive qualities within even the smallest parts of a system.

When comparing manufacturers, we look to the advice and guidance from the National Cyber Security Centre (NCSC) to define best practice.

A strong cyber vendor is one who:

- Designs cyber protective measures into all parts of their system
- Aspires to meet robust credential standards, such as MIFARE DESFire EV2 and the FIDO Alliance specifications
- Has empathy for the IT security professional with a security hardening guide, allowing them to mitigate risks they deem important
- Solves business problems across a wide range of areas in your business – a business integrated security solution, not just a solution to open and close doors
- Undertakes regular internal and external penetration testing to ensure solutions are hardened and secure
- Aspires to be a CVE Numbering Authority, which grants the authority to publish security vulnerabilities identified within their own product suite
- Offers a security health check to assist sites with identifying and responding to any vulnerabilities



When it comes to high security solutions, there are six critical success factors to look out for.

Encryption and authentication

End-to-end encryption protects against installer and insider attacks. Encryption and authentication should be built into a system. Done well, an adversary will look for an easier target.

Assured compliance

A government-assured compliance sets the benchmark and ensures products stand up to regional security standards, such as CAPSS (Cyber Assurance of Physical Security Systems) in the UK.

Ease of use and control

High security systems should be simple to operate, while providing rich and detailed information that allows security officers to effectively handle any security incidents.

Secure devices

It is essential to protect the secret keys for encryption and authentication. Best practice is the use of hardware key store modules in the devices that make up an access control or intruder alarm system. Proof of origin for electronic devices in a system is achieved by Certificates and serial numbers loaded in the manufacturer's factory to protect against supply chain and substitution attacks.

Ease of patching

Eventually, security vulnerabilities will be exposed in every software system as techniques and technologies evolve. It is essential that software and firmware are able to be updated over the network, quickly and efficiently.

Security hardening guide

A high security hardened system will ideally use at least two-factor authentication. Computer networks will be encrypted, and there will be regular rolling of keys, authentic hardware checks, and encrypted end of line modules.

Why consider a government-approved security solution?

Government-approved security solutions have a history in the high security space, with solutions meeting global standards, including AACS and CAPSS in the UK, Type 1A in Australia, and FIPS-201 standards in the United States. There are also higher grades of other security standards, which are not government standards, but which define regional security requirements, such as the intruder alarms standard EN50131 grade 4 which is only achieved by a small number of security solutions.

In the United Kingdom, the National Protective Security Authority (NPSA) works alongside the NCSC to help reduce vulnerability to terrorism and other threats. NPSA is the lead authority for physical security while NCSC leads on all things cyber. Together, they work with manufacturers to develop more secure, robust, and cyber-assured products that help protect corporate data and assets.

As technology has advanced and become more interconnected over the years, the way organisations do business has changed dramatically. Your security solution may not have been designed to manage all the things it does now. Third-party integrations, connected devices, and even the external networks employees connect to while working from home, all create a risk of cyber breach.

Through testing their products against rigorous government standards, manufacturers offer organisations peace of mind that their solutions are resilient and fit for purpose.

The Five Eyes alliance

The Five Eyes alliance comprises of five countries – Australia, Canada, New Zealand, the United Kingdom, and the United States – who are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence.

To meet government standards issued by nations within the Five Eyes, security manufacturers must produce solutions capable of passing aggressive tests and meeting the highest standards. Achieving compliance is a testament to a manufacturer's strength in security, and companies and organisations can be assured that these solutions are capable of protecting against both cyber and physical attacks.

Industry opinion and views

According to **Steve Bell, Chief Technology Officer at Gallagher**, "Gallagher has delivered systems to meet government compliance standards over more than 15 years and each standard mitigates a set of risks that is important for the eco-system of that government. Gallagher has learnt a lot from these standards and has incorporated many of the techniques and technologies into our designs for all our customers."

Gallagher works closely with a number of cyber security experts and organisations, some of whom shared their views on what government-approved platforms mean to users and why commercial organisations should consider using them.

Kevin Brownell, Partner, PTS Consulting wonders why you *wouldn't* consider a government-approved platform. If a solution is tested to the highest standards, Kevin suggests you need to think about the level of risk you are exposing your organisation and your clients to without it.

Matt Brittle, Head of Security, Risk and Resilience at WSP, believes there are some misconceptions in the industry in regards to cyber and the use of government-approved solutions in commercial settings. "There's still a misunderstanding that when you talk about cyber, you're talking about ones and zeros going down cables, and not the physical security of devices."

Ellie Hurst, Head of Marcoms and Media at Advent-IM Ltd, believes end-users are starting to understand the commercial possibilities afforded to them when they introduce solutions that have attained government-level cyber security standards.

Ellie states, "When we look at our lives today, we realise that everything is interconnected." Poorly configured systems, neglected maintenance, and matching different technologies together creates gaps and vulnerabilities that are often the most frequently exploited. End-users are now looking for more assurance from their security solutions to ensure they aren't vulnerable, or creating a vulnerability for someone else.

Scott Wiener, Technical Director & Head of Service Line, Atkins Fellow, Security believes the boundary between high security and commercial organisations has moved this year. "Where is the boundary? It's certainly moved. What's a priority asset now?" He sees a need for organisations to adapt quickly and make access control more mobile.

What does the future look like?

The COVID-19 pandemic created a shift in the way we work. With many employees no longer tied to desks, the world is our workspace – people work from home, in a coffee shop, on a train, or in the office. This brings an increased element of risk and new challenges for securing individuals and protecting the data on networks they connect to.

More people consider the risks things such as IoT, remote working, and third-party devices present to organisations. As the risks grow, robust security solutions that meet government standards have become more commonplace in the commercial world as organisations look for solutions capable of providing protection against ever-evolving threats.

References

[1] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[2] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[3] https://www.ibm.com/uk-en/security/data-breach

[4] https://www.csoonline.com/article/3440069/ukcybersecurity-statistics-you-need-to-know.html

[5] https://blogs.microsoft.com/on-the-issues/2019/09/26/cyberpeace-institute-fills-a-critical-need-for-cyberattack-victims/

[6] https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

Want to know more?

Visit **security.gallagher.com** for more information on high security solutions or email us:
UK / Europe: **info.eu@security.gallagher.com**   Global: **security@gallagher.com**

GALLAGHER™
Security