SENETAS
Security without compromise

CYBERSECURITY CONSIDERATIONS FOR THE DEFENCE SCIENCE AND TECHNOLOGY SECTOR

TO GO BOLDLY, AND SECURELY

Year after year we witness a seemingly inexorable increase in data breaches. In 2018 alone, almost 5 billion records were lost or stolen.

We all understand the negative impact of data loss, so why is it that so many organisations seem to be failing in their duty of care to protect sensitive personal and commercial data?

Failure may sound harsh, butshareholders, suppliers, customers and employees have a right to expect their data to be protected. They shouldn't expect to suffer harm (loss of share capital, business disruption, stolen IP, privacy breaches and financial penalties) as a result of inadequate cyber-security.

High-tech industries have become a target of choice for "bad actors" because of the potentially rich rewards resulting from a successful hack.

The defence science and technology industry is not immune to a diverse and evolving threat landscape that features state-sponsored hackers, cyber-terrorists and organized cyber-criminals.

Threat vectors are as diverse as they are numerous; from systems and network hacking to malicious code (malware) embedded in seemingly innocent content and sophisticated eavesdropping technologies.

Whether these attacks are aimed at stealing high-value data, damaging systems or crippling national infrastructure, the need for enhanced cybersecurity prevention and protection technologies has become a core business imperative.

A NEW FRONTIER FOR CYBER-THREATS

The global defence science and technology industry has seen steady growth in recent years. According to recent reports from Deloitte and PWC, the industry's value is approaching US$800billion.

If we include the wider aerospace sector, it brings the value closer to US$1.4trilion – a valuation that Carnegie Mellon expects to double to US$2.8trillion by 2028. Whilst criminals will always follow the money, there are other bad actors with more nefarious purposes in mind.

Defence science and technology businesses are positioning themselves to make the most of the opportunities an expanding and maturing market represents. However, as they do so, bad actors are poised to take their own advantage.

The technical and collaborative nature of defence programs generates large volumes of proprietary and operation data, much of which will be sensitive in nature. This data is an attractive target for cyber-criminals.

Threats may vary from eavesdropping and IP theft to rogue data injection and access control. The impact of a successful data breach could range from financial (in the event of a loss of proprietary IP) to existential (in the event of an aborted or sabotaged program).

Strong and effective cyber-security prevention and protection technologies are readily available, and more cost-effective than ever. For example, the use of strong encryption solutions (both for data at rest and in transit) is considered mandatory by many cyber-security experts. Encryption should be considered an everyday part of doing business; especially in high-value and high-tech industries.

Strong encryption is the only assurance against a successful data breach, protecting the data itself against theft, authentication or manipulation.

The defence industry must also prepare itself against the evolving cybersecurity landscape, in particular the threat posed by quantum computing. Contemporary systems will be rendered ineffective in the post-quantum era. New encryption algorithms and technologies will be required to provide quantum resistance.

Ironically, as we move towards the age of the quantum computer, cyber-security professionals are turning to the defence industry and its satellite technology for the answer to tomorrow's cryptographic technologies.

Quantum Key Distribution is a technology that sits at the heart of future quantum communications networks. A network of communications satellites could hold the answer to a cost-effective, global QKD platform.

IF YOUR DATA'S WORTH ANYTHING, IT'S WORTH ENCRYPTING

Thales' breach level index reports that over 14 billion data records have been lost or stolen in the past 5 years. Worryingly, less than 4% of this data was protected with encryption. The EU's General Data Protection Regulation (GDPR) was introduced in 2018.

In it, a qualifying breach is deemed to be on in which "…data is not protected by strong encryption…".

As the gold standard of data security regulations, the GDPR introduces unprecedented data breach notification requirements and the potential for severe financial penalties in the event of successful breaches of unencrypted data.

The GDRP is important to the global defence industry because it doesn't just apply to organizations within the EU, but anyone who trades or collaborates with EU member states.

Despite Australian data privacy regulations and federal government defence supplier data security requirements, in October 2017 it was revealed that a breach of a Defence Industry contractor's data lead to the theft of 10 gigabytes of sensitive data.

This was reported to have included information on the F-35 joint strike fighter, C130 Hercules aircraft, the P-8 Poseidon surveillance aircraft, joint direct attack munition (JDAM) smart bomb kits and several naval vessels. None of the data was encrypted.

Cyber-security is not simply about protection against data loss or privacy breaches.

Of increasing concern is the risk of data manipulation, access control, injection of rogue data and even interference with industrial and other asset control systems (i.e. critical national infrastructure including satellites).

The impact of a data breach or cyber-attack in some commercial markets can range from minor inconvenience to financial hardship; from the temporary shut-down of an application long-term reputational damage.

For critical infrastructure and hi-tech sectors of national importance, like the defence industry, the stakes are far higher.

A successful hack of an unencrypted network could enable a bad actor to seize control of a launch vehicle or orbiting satellite and either abort the launch or bring the asset crashing back to earth. Strong encryption also protects against these acts of cyber-terrorism.

In the words of cyber-security expert and cryptographer, Bruce Schneier, "Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting."

TRAPS FOR THE TRUSTING

US author and consultant Denis Waitley said, "Life is inherently risky. There is only one big risk you should avoid at all costs, and that is the risk of doing nothing." His words are more poignant in a world where the technologies that help drive business opportunities also open doors to cyber-security threats that will undermine them.

The adoption of new business technologies and collaboration (local and global) among high-tech organisations (partners, customers, suppliers) using Cloud, SaaS, multi-Cloud, IaaS and hybrid-Cloud technologies continues to accelerate. Significantly, they require more complex and high-performance data networks than ever before to enable them and transmit record volumes of proprietary and control systems data.

The world we know has become dependent upon high-speed data networks. From the outset, these data networks are not inherently secure; and networking devices such as routers and switches often add security vulnerabilities. A reliance on basic infrastructure to secure network data in motion is effectively "a trap for the trusting".

We all live in a connected world, where information is digitized, transported and exchanged across wide area networks. It is the digital nature of this information that exposes it to additional risks in the form of malware or malicious embedded content.

Cyber-security should not be limited to protecting data at rest. In January 2019 Adam Kujawa, Head of Malware Intelligence at Malwarebyte, published a report.

In it, he highlights the findings of his research into state-sponsored threats, as well as threats to government and private industry. He explains that cyber-criminals are focused on profitable targets - businesses whose data networks are unsecure (unencrypted) – with information theft as the primary objective.

McKinsey & Company's James Caplan emphasizes that network transmitted data is a cyber-criminal's main target. He argues that the sheer volume of data moving across networks enables theft of gigabytes of data in minutes. He said, "The larger the data volume, the greater the risk."

Of equal concern to any organisation is the potential for any file entering and moving across its networks to contain hidden threats that, if released could bring down systems and hold the business to ransom.

Whatever the threat, it's clear that failure to treat cyber-security as a core business enabling technology, rather than as a side issue, risks catastrophic damage and potential litigation. High-tech IP-driven organisations arguably have the most to lose.

AN UNSETTLED OUTLOOK, THE CLOUDS ARE GATHERING

If cyber-security is tough today, it will be much tougher tomorrow. Emerging business technologies promise greater security challenges as the Internet of Things (IoT), borderless infrastructure and ubiquitous cloud applications lead to a further explosion in high-speed, high-performance data networks and transmitted data volumes.

The defence industry's use of emerging IoT and AI technologies, and its collaborative use of public and private cloud infrastructure, introduce new vulnerabilities.

Whilst identity theft and financial account access are major motivators for cyber-criminals, state-sponsored cyber-attacks and hacktivism pose a larger threat to society as a whole. Nuisance hacks are becoming less prevalent, but we are seeing the emergence of cyber-terrorism as an existential threat.

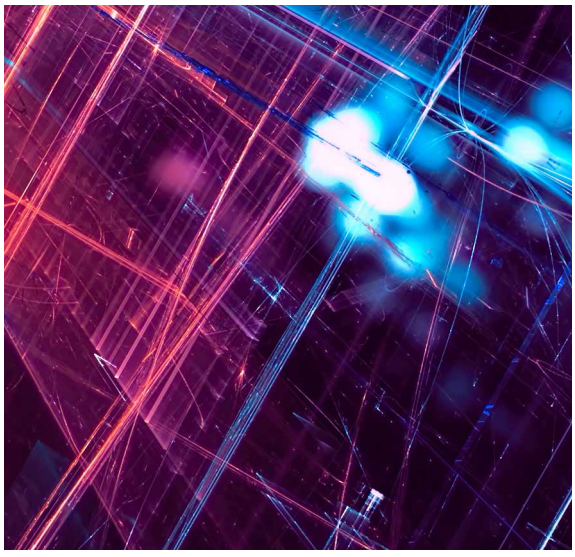
PREVENTION AND PROTECTION - CAVEAT EMPTOR

There are two key components to data security, prevention and protection.

Prevention technologies (e.g. firewalls) attempt to stop cyber-attacks and data breaches from occurring. They are essential components of a good cyber-security strategy but cannot work alone. If there is one truth in data security, it's that it's not a matter of if a data breach will occur, but when.

Protection technologies (e.g. encryption) secure the data in the event of a breach or attempted manipulation. Only strong encryption ensures that when prevention security fails, the breached data is rendered useless in the hands of unauthorised parties.

Remember, not all cybersecurity solutions are created equal. Your choice of technology should be fit-for-purpose. If you want to ensure long-term protection beyond the useful life of the data, it needs to be purpose-built, with the agility to adapt to future quantum cryptographic technologies.



ENCRYPT EVERYTHING

Four main factors have added to cyber-security risks in recent years; vulnerable network devices (routers and switches); sharing of unsanitised and unencrypted documents with third parties (customers, partners and suppliers); and innocent human and technical errors.

Whether all data in an organisation is sensitive is not the point. As Schneier emphasizes, nor is it a reason not to encrypt.

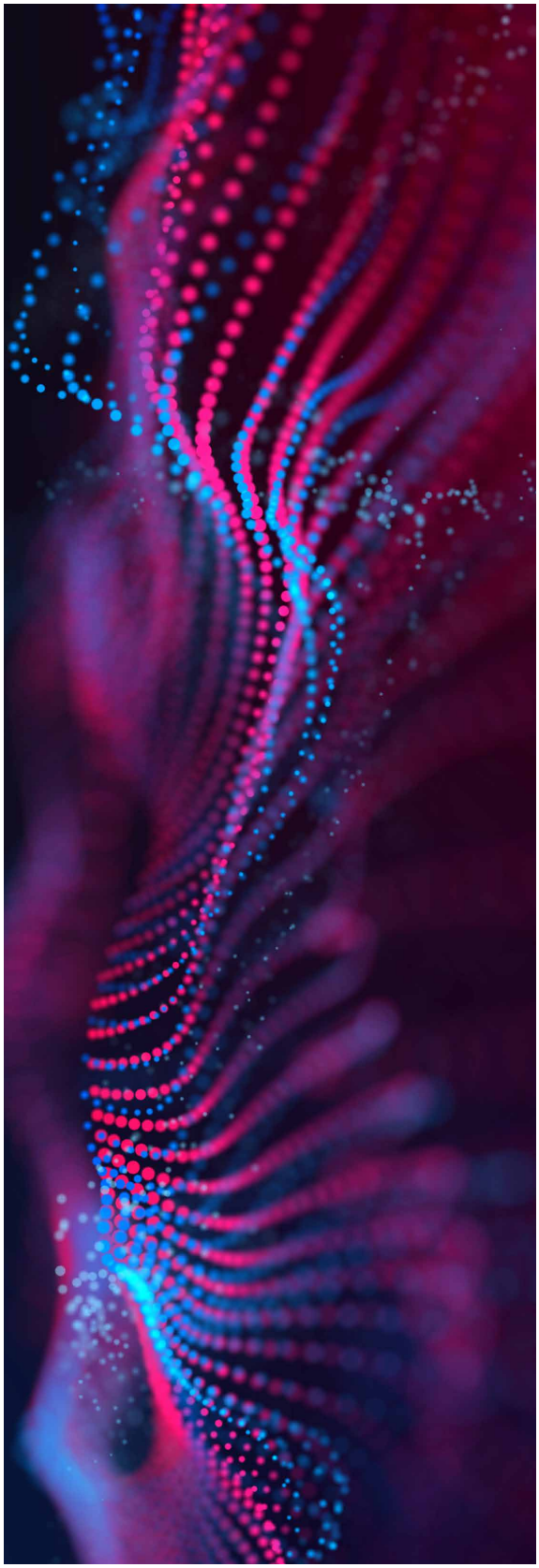
Data has become the currency of modern business and the rewards for cyber-criminals, rogue-states and industrial-spies are significant.

Eavesdropping, theft of IP and widespread use of malware could have catastrophic implications for defence industry organisations, shareholders and customers alike. US industrial software developer AMSC – a listed company – discovered that critical software IP was stolen and used by foreign competitors.

Despite swift action (and help from the FBI) AMSC's stock value fell from $370.00 per share to just $5 per share while the matter was being prosecuted.

To help provide a framework for best-practice, state and national institutions across the globe are introducing new guidelines to help protect our most valuable and vulnerable digital assets.

However, the question remains, how will the defence industry address its need for optimum cyber-security?



GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its brand.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our **ANZ Partner Page** for full details.

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file-sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	T: +65 8307 3540	E: infoasia@senetas.com
Australia & New Zealand	T: +61(03) 9868 4555	E: info@senetas.com
Europe, Middle East & Africa	T: +44 (0)1256 345 599	E: info@senetas-europe.com
The Americas	T: +1 949 436 0509	E: infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has an encryption solution to suit. Our certified high-assurance encryptors protect data across networks operating at speeds from modest 10Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 5Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

SECURE FILE SHARING

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

XXXXXX-XX1020

SENETAS