White Paper

Predictions 2020

Looking forward to next year in cyber security

Huntsman®
Defence-Grade Cyber Security

Predictions 2020

Looking forward to next year in cyber security

Each year Huntsman Security provides its views and estimates on what the big topics, main drivers and pressing concerns will be in the cyber security and related fields for the coming year.

> “Transformations often take longer than 12 months to be identified as necessary, to be executed and to become established.”

This year there are some common themes that endure, so we’ll highlight these as “work in progress”. Transformations often take longer than 12 months to be identified as necessary, to be executed and to become established.

However, there are other themes emerging through a combination of drivers from audit, compliance security and governance that are now showing signs of influencing the way that cyber risks are managed in a much shorter timescale.

Huntsman®

1 Growth in the MSSP market

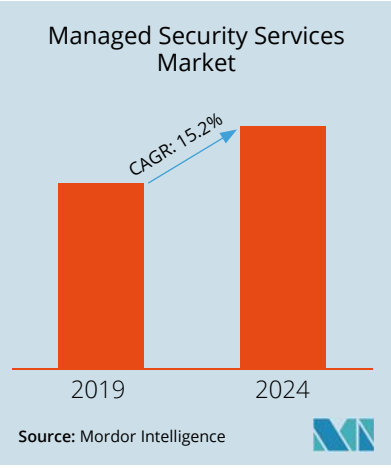
Predicting growth in the managed security services market has been a recurring theme of Huntsman Security's predictions reports. We don't see this trend abating any time soon as businesses increasingly struggle with growing cyber threats foisted upon teams that are constrained by resource and skills shortages.

We are not alone in this prediction[1]:

- **Markets** and Markets expect it to "grow from USD 24.05 billion in 2018 to USD 47.65 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 14.7%".
- **Mordor** Intelligence put the CAGR at 15.2% (see chart)
- **Reuters** reports that "The Managed Security Services Market is growing rapidly over 12% of CAGR [to] USD 34 Billion by the end of forecast period."
- **MarketWatch** make a similar forecast: "The Global Managed Security Services Market is expected to exceed more than US$ 58 billion by 2024 and will grow at a CAGR of more than 14.5% in the given forecast period."

Small businesses are usually ill-equipped to deal with advanced and organised cyber threats and often their technology is outsourced to hosting companies, cloud providers, development teams etc. It is inevitable that security monitoring, threat detection and incident response follows the same model.

All MSSPs, even those that specifically target small and medium enterprises (SMEs), will want to grow their own business – that means finding more customers (and hence having keenly priced entry-level services) AND having a portfolio of value-added services they can offer on top. Many are also seeking to spread into bigger customer environments. So this market growth will compromise additional services to new and existing customers as well as through mid-size and larger businesses increasing their adoption of MSSP services.



1 https://www.marketsandmarkets.com/Market-Reports/managed-security-services-market-5918403.html
https://www.mordorintelligence.com/industry-reports/security-managed-services-market
https://www.reuters.com/brandfeatures/venture-capital/article?id=79915
https://www.marketwatch.com/press-release/managed-security-services-market-is-expected-to-exceed-us-58-billion-by-2024-2019-02-27

2 RegTech will drive the "digital transformation" of compliance

RegTech is the use of technology to ensure businesses meet their regulatory and compliance obligations. It originated in the financial sector where banking rules around things like anti-money laundering (AML) and "know your customer" (KYC) designed to prevent fraud, theft, loss and other illegalities have led to additional regulatory burdens on financial institutions.

In the cyber security space, we have seen the rise of automation (security orchestration and automated response) for a while in threat detection and response.

However, the regulatory burden is increasing for CISOs and audit teams too, so this is driving this same approach to controls monitoring, audit and assessment while dealing with the scarcity of security resources – i.e. using RegTech to automate assurance in the cyber security framework that is in place.

As threats increase and regulatory burdens (such as GDPR, Open banking and PSD2) continue to magnify the scale of risks, we predict continued adoption of RegTech solutions across all sectors. This will help to ease the audit burden by analysing and making decisions about the state of cyber risk management, and in some cases launching workflows to resolve issues that have been identified.

3 Privacy and security risks will become reputational rather than technical or financial

There is no doubt that privacy and security breaches have financial impacts (just ask BA[3] and Marriot[4]). This can include the monetary losses through fraud, costs of communicating to affected customers, credit/identity theft insurance, consultant's fees to investigate the breach, the well-publicised regulatory fines, PR costs, legal fees as well as marketing costs to rebuild a damaged customer base.

The value of "reputation" is much more keenly felt by businesses as something that can be irrevocably damaged. This is not limited to security – it can be due to services shortcomings, environmental impacts, labour practices, paying taxes or boardroom tangles.

"Data custodianship" – or how responsibly and carefully people's personal data is treated – is increasingly a part of corporate social responsibility that cannot be ignored. The rise of customer boycotts, social media and activism means that failures can be hard to recover from – and this trend for citizen power in the face of corporate failings will continue to be a factor in 2020.

2 https://www.huntsmansecurity.com/wp-content/uploads/2018/07/Infographic_PSD2.pdf
3 https://www.huntsmansecurity.com/blog/once-more-unto-the-breach-the-ba-gdpr-fine/
4 https://www.huntsmansecurity.com/blog/cyber-security-marriott-gdpr-breach-fine/

4 Risks will be measured by business outcomes and compliance will be a means to an end

Risk management is often linked to compliance standards - either legislative and mandated or specifically chosen. Compliance to a security standard helps manage risk as there is an externally defined framework for security management and controls. Many compliance standards (ISO 27001 is a good example) require you to conduct a risk assessment in order to derive a list of controls that are applicable to your environment.

One common challenge is that the list of controls selected according to the risk assessment is "most of them". A few might not be appropriate or too expensive, but most "standard" sets of good practices, are just that – standard.

Risk assessments typically highlight the relative importance of controls in risk terms, in theory driving the order in which they are implemented or their priority. However, to be compliant you need a wide range of controls and have them all generating evidence.

"One common challenge is that the list of controls selected according to the risk assessment is "most of them". A few might not be appropriate or too expensive, but most "standard" sets of good practices, are just that – standard."

As this decade ends, we are seeing compliance being driven less by academic goals and more by business needs. The heightened regulatory environment discussed above, as well as the continued push to secure supply chains and third parties, remains a challenge.

The UK has had some success with Cyber Essentials, likewise there are equivalent approaches for Australia (Essential 8), US and other governments.

The outcomes in terms of reduced reputational risk due to embarrassingly "trivial" failures, greater assurance in supply chains and reduced insurance premiums is now on the business balance sheet.

Reduced cyber insurance costs, is perhaps the most obvious driver. Businesses might save money by not investing in a control, and they might not have to pay out for a breach if they are lucky and one doesn't occur - so "bad security" can be cheaper than "good security", if you get away with it.

However, if companies are required or have decided to have cyber insurance, their premiums will be higher if security is poor. The business outcome of reduced premiums is a real and constant cost that can much more directly feed a financially-driven security business case.

5 Acquisition/Merger due diligence will receive a boost

There have now been two big high-profile cases where cyber security has been the centre of attention for mergers and acquisitions.

The first was the purchase of Yahoo by Verizon. Yahoo had a breach and Verizon found out about it (along with the rest of the world) before the transaction had completed. As a result, Verizon saved themselves £350m and Yahoo took a hit.

The second was Starwood who also had a breach. This time Marriot didn't find out during due diligence prior to acquiring Starwood which cost them a fine of £100m from the UK Information Commissioner's Office.

https://www.theweek.co.uk/cyber-crime/98262/marriott-starwood-data-breach-what-happened-are-you-affected-claim-compensation-share-price

These two examples indicate there will be greater emphasis on cyber security due diligence during these sorts of transactions. Three obvious angles for this are:

- **Has the deal target already suffered a breach that constitutes unspecified financial liabilities?**
  - Is there a smoking gun?
- **How likely are they to have suffered a breach that has not yet been identified?**
  - How good is their cyber hygiene?
- **What risks do their systems pose to the acquirers when they are connected?**
  - Is this a third party we would normally be happy to link up with?

We predict acquirers will have to increase investment in cyber security as part of their value appraisal of potential targets to avoid incurring later costs (or fines) of hundreds of millions of dollars should they omit or miss something.

6 Cyber insurance will evolve

In the US, cyber insurance is buoyant and driven by mandated data breach notifications where costs and pay-outs have been easier to quantify than the fines and sanctions imposed by regulators in other countries.

For many businesses (and insurers) there are challenges. How big should premiums be for a given risk, how do we quantify risk (for the insured party and underwriter), what level of diligence and assessment is appropriate – questionnaires or some form of direct external or internal assessment?

For the market to grow further (especially outside the US) these types of questions will need to be answered. We have seen signs that the use of technology and more actuarial approaches are starting to be adopted in the global cyber insurance industry.

Increasingly insurers will want to deploy "black box" type security measurement and telemetry solutions to monitor cyber risks to keep premiums low (and make pay-outs less frequent), reduce the overhead of scrutiny and to better understand changing risks from cyber hygiene.

The view that cyber insurance is a control that can deployed in lieu of security investment, that you can save money on controls if you have good insurance, is being seen as the myth it is; underwriters do not underwrite 'unknown' exposure.

It is self-evident that for the market to function for both sides, there must be some level of control otherwise the premium will be prohibitively high. Spending on recognised controls can be offset against reduced premiums as well as losses and impacts that occur. Particularly as the cost of a loss is only incurred when it happens, but an insurance premium is paid every year irrespective; any reduction is a guaranteed saving rather than a potential one.

Businesses can either pay for insurance (a definite lower cost) or risk a loss (higher potential costs if it happens). Mandation of cyber insurance may change this overnight if a regulator, government or large supply chain decide it is appropriate.

Huntsman®

7 Audit rules will drive greater automation

The rules around corporate audits go beyond just the cyber security remit; encompassing financial reporting and exchange filings, as the role of boards and the information provided to stakeholders, regulators and investors is improved.

We've seen the requirement to record and report cyber security risks and breaches in reports and filings for some time. The cyber security threat is firmly on boards' agendas, and it is increasingly common for audit functions to look in detail at cyber hygiene or risk exposure that businesses have as part of their internal or external audit programme.

> "As audit scopes grow to encompass cyber security, the process of audit itself has been striving for improvements."

There is an imperative to establish the status of controls and the level of trust in systems and to ensure that risks and breaches are accurately quantified and reported where they might lead to financial liabilities or costs.

As audit scopes grow to encompass cyber security, the process of audit itself has been striving for improvements. The latest US Public Company Accounting Oversight Board (PCAOB) rules now require auditors to report not just on the level of assurance in controls, but also in the availability and timeliness of evidence and the amount of human interaction between the systems and the audit function.

This means identifying the risks that a control could fail and go unnoticed or, worse, could be concealed. The improvements aim to reduce the chance and scope for misstatement – either accidental or deliberate - through not having accurate control performance data.

Technology is being increasingly used to speed up audits, to make control measurement continuous and minimise human influence in data gathering and analysis to reduce the overhead and risk of interference.

Gartner have invented a term – CARTA (Continuous adaptive risk and trust assessment). However, hot off the back of "Fintech" the wider industry is using the term "RegTech" for the wider compliance technology solution area. We predict this broader term will predominate and we will increasing see RegTech audit solutions addressing cyber security challenges.

See Investopedia's definition here:
https://www.investopedia.com/terms/r/regtech.asp

8 Skill shortages will continue

A year is too short a period to alleviate a skills shortage, such as in cyber security. It is a multi-year, longer term challenge involving training, schools, academia, promotion and growth in professionalism for people moving into the sector from other related roles.

Increasingly we are seeing a dynamic where the demand for skills is not just for "security" but for those who have a wider view across cyber risk and the areas elsewhere in the business to which it relates. Multi-skilled individuals will be increasingly scarce, and it will become particularly evident in the short term as cyber risk interfaces more directly with compliance, audit, marketing and other business functions.

Expect to see demand for security teams that better understand the wider business risk landscape (as well as security risk management), for privacy and security managers that can shape their strategies in terms of marketing and reputational endeavours, for IT staff that can understand the point of view of audit (and vice versa) and for cyber security operations teams that will understand and see audit as a beneficial arbiter, rather than an overhead.

9 Supply chain risks continue to get focus

The risk posed by "supply chain" cyber security has never been in sharper focus. Numerous breaches have occurred resulting from lax third-party protection of data and the rise of regulations that enforce greater diligence (such as in GDPR), means this is a well-established problem.

The audit side of this has been maturing for a while, the SAS70 process for supplier audit and the SOC2/3 methodologies for auditing service providers continue to evolve. In parallel, various government run schemes or standards have been defined – FedRAMP (US), Cyber Essentials (UK) and Essential 8 (Australia) – to allow agencies to gain more universal assurance from those that service them.

In the Defence sector, the US have been developing a "Cybersecurity Maturity Model Certification" (CMMC) approach for their defence supply base. Version 1.0 of the framework will be available in January 2020 and by June, defence suppliers should begin to see these requirements in RFIs.

In 2020 we predict greater international efforts to unify this assurance process so that multinational suppliers have one common set of hoops to jump through rather than several separate ones.

Huntsman®

10 Continued attacks on "Society"

Huntsman Security has previously outlined the threats to elections through cyber-attacks on voting systems, electoral rolls and through social media disinformation and propaganda.

In addition to that, past years predictions around the risks to CNI persist. Despite the NIS directive in the EU and a push to raise cyber security hygiene standards in the Australian market there is still a clearly perceived risk that big, important systems and networks that society depends on could be attacked.

The risk of destabilisation of society (either through direct attack or social media) must be seen in this context. You don't need to influence or change a government to shift public opinion or public policy. You may not need to cripple the networks of real-world systems; you may just need to sway people's views.

> "You may not need to cripple the networks of real-world systems; you may just need to sway people's views."

With the comprehensive resources and apparatus at their disposal, there are foreign powers who will continue to use this approach to target societies. Vaccinations, fracking, race relations, public scandals, the perception of danger from terrorist or religious groups or immigrants – all these things can be stirred up in a way that damages the cohesion of communities. Sadly, we don't see this changing in 2020.

Huntsman®

Finally...

"20/20 Vision" will be an over-used buzzword

In security, we often talk about the ability to see threats coming, or to detect attacks, or to gain better oversight over the activities on our networks and the systems we protect. It is all about visibility.

The effort put into detection solutions, AI, reporting and dashboards means that marketing teams will be unable to avoid the temptation to draw pictures and write copy linking that ambition to measurements of human vision. Blog posts, white papers, product and service literature discussing and promising "20/20 vision" in the coming year is something we are going to have to put up with for the next 12 months; until 2021, when we can use "20/20 vision" to refer to what has transpired in the past (with "20/20 hindsight").

Talk to Huntsman Security about your cyber security monitoring and measurement

For a detailed discussion on monitoring and measuring your cyber risk, please contact the appropriate office listed below.

About Huntsman Security

Huntsman Security is the trading name of Tier-3 Pty Ltd. The technology's heritage lies in delivering a key foundation stone of the cyber security risk management, monitoring and response capability in some of the most secure and sensitive environments within the intelligence, defence and criminal justice networks across the world, where Huntsman Security solutions are deployed and accredited to the highest security levels.

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street, Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman