dimension data

NTT

Executive Guide to the NTT Security 2019 Global Threat Intelligence Report

Cybersecurity insights from the inside

Insights **driven by data**

Contents

Foreword

For several years, Dimension Data has published an Executive Guide to the NTT Security Global Threat Intelligence Report, providing insights and analysis from our cybersecurity experts about the shifting threat landscape. We also provide you with best practice guidance, and practical measures you can take to bolster your cybersecurity defences.

Security's a journey, not a destination

Now, more than ever, cybersecurity teams are seeking to become more agile. They help organisations meet regulatory compliance requirements, align to industry best practices, and accelerate business transformation initiatives. Effective cybersecurity acts as a business enabler – building customer, shareholder, and employee trust. This enables organisations to protect and enhance their reputation and reduces the risk of the many negative consequences of a cybersecurity breach.

By providing value to the business, cybersecurity helps differentiate in an otherwise crowded marketplace and improves users' and customers' experience. From on-premise IT; mobile devices; connected operational systems; to public, private, and hybrid technology deployments; cybersecurity leaders need the confidence that their infrastructure and data are adequately protected.

This year, for the first time, we've included additional findings and recommendations on cybersecurity maturity and preparedness in our Guide, based on insights drawn from our Cybersecurity Advisory consulting service engagements with clients across the globe.

We look at the global threat intelligence gathered by our teams and examine it through the lens of industry maturity and preparedness. We evaluate how well equipped organisations are to deal with the ever-evolving threat landscape, based on their current and desired levels of maturity, as seen through our global footprint.

Encouragingly, we can confirm that C-level leaders are becoming increasingly aware of cybersecurity and more cognisant of the threat landscape, compliance, risks, and technology innovations. This helps them to identify their focus areas, priorities, and investment decisions. We also see organisations accelerating their security transformation by forging strategic relationships with select partners to build security roadmaps and architectures and optimise their infrastructure – all aligned to their unique business needs.

This Guide is essential reading for executives seeking to improve their own organisation's resilience and embark on the journey to world-class cybersecurity.

Mark Thomas

VP, Cybersecurity — Dimension Data

For the past 18 years, Mark has worked in the cybersecurity field establishing pragmatic, business-aligned risk minimisation strategies and developing intelligence-led computer network defences. His broad knowledge and in-depth expertise are a result of working extensively in consulting, technical, and managed services with large enterprises across numerous industry sectors including finance, government, utilities, retail, and education.

7 key insights into the cybersecurity landscape

A high-level overview of the most prevalent threats, motives, and malicious actors observed over the past year, their impact, and recommendations to improve your cybersecurity maturity to bolster your defences.

1. New dawn rising in the fight against cybercrime

The fightback against cybercrime is gathering momentum, and attracting board-level interest. While the threat landscape will continue to evolve, and the emergence of new, more sophisticated vulnerabilities and attack vectors is inevitable, we should be optimistic about the future of the fight against cybercrime, for three key reasons:

- **Predictive threat intelligence is reaching new heights.**
- **Organisations' security investments are becoming more informed, targeted, and strategic, and cybermaturity benchmarking is gaining popularity.**
- **We're seeing increasing buy-in and collaboration among stakeholders across the entire cybersecurity value chain.**

Engage with providers who're invested in and understand your business, and how they can help drive it forward by applying security holistically throughout the lifecycle, from development to operations, as part of a long-term journey. This will help you chart your course to safety.

Read the full article **here.**

2. Vulnerabilities surge – and weaponised

During 2018, there was a 12.5% increase in the number of new vulnerabilities discovered. 'Weaponisation' of vulnerabilities is also on the rise. Here, cybercriminals exploit vulnerabilities to launch highly co-ordinated attacks against individuals, businesses, and specific groups by using a combination of technical and non-technical tools. Often these vulnerabilities are targeted via automated exploit kits.

Over the last year, many vulnerabilities were discovered in older software that have been present for years. Others exist in common systems, utilities and applications, and application code libraries used to support daily operations.

Be honest with yourself about your current state of cyberpreparedness and vulnerability management capabilities. Formulate a plan and roadmap, which is business-led – rather than technology-driven – and identifies your immediate priorities, to move you from your current to your desired state.

Read the full article **here.**

3. Cryptojacking: 'compute to cash' rises

Cryptojacking is also is known by several other names, including coin mining, cryptomining, and cryptocurrency mining.

Not all cryptomining activity is unlawful: a user may install a coin mining programme on their personal system to generate cryptocurrency for themselves, using their own computing resources. But it becomes illegal when they use someone else's resources – CPU power and energy – without their knowledge or permission, to mine cryptocurrency for their own financial benefit.

In 2018, cryptojacking, while still in its infancy, caught many organisations off-guard and represented a significant amount of hostile activity.

Protect your organisation from the threat of cryptojacking by applying 'least privilege' controls and implementing egress and ingress filtering restrictions, as well as browser plugins to limit site functionality. Also, deny Stratum protocol usage, and segment your network environments.

Read the full article **here.**

4. Credential theft: 'handing over the keys to your kingdom'

Credential theft isn't a concept that's new to most people – but in the context of cybersecurity, it's become increasingly prevalent over the last few years.

Credentials are the 'keys to your kingdom', protecting your organisation's networks and data from unauthorised access. This makes stolen credentials a valuable target for threat actors. Our observations reveal that phishing and malware are cybercriminals' techniques of choice when it comes to launching credential theft campaigns. And we're seeing a spike in the number of credential theft attacks targeting cloud platforms.

Successfully fending off credential theft attacks on your business involves implementing multi-factor authentication, segmenting your network environment, and enforcing 'least privilege' and segregation of duties. Other recommendations include implementing network activity monitoring and data loss prevention, and educating your employees to be vigilant about phishing attacks.

Read the full article **here.**

5. Web-based attacks moving up the stack for profit

Web-based attacks aren't new and have been frequently observed for some years. However, we've seen an alarming increase in recent cyberattacks in this area. In fact, they doubled year-on-year, (accounting for 32% of all attacks detected during 2018), and represented the top type of hostile activity.

Web-based attacks target web-application and application-specific vulnerabilities in technologies frequently used by many businesses. Any organisation that has a web presence is exposed to these attacks … and the larger their web presence, the greater the attack surface. Compounding the challenge is that today, more companies' applications are being housed in the cloud which exposes the organisation to new attack types.

Our advice to help protect yourself from web-based attacks includes prioritising patching, segmenting your network environment, and enforcing secure coding practices. Also consider deploying application-aware firewalls and performing regular vulnerability scanning.

Read the full article **here.**

6. Compliance firmly on the boardroom agenda

Regulatory compliance is a well-known IT risk management challenge faced by many organisations. Last year, data protection and privacy dominated media headlines, spurred by the introduction of the General Data Protection Regulation (GDPR) which came into effect in Europe in May 2018. This caused a stir globally regarding data protection principles and personal privacy rights.

Subsequently, a number of other countries have implemented new data protection regulations or are 'beefing up' their existing compliance frameworks and regimes.

Data protection principles and personal privacy rights should put cybersecurity firmly on the boardroom agenda.

Ensure that executives understand how cybersecurity and data protection can deliver (or, if ignored, can potentially erode) tangible business value. This will gain their attention and buy-in, and help secure the appropriate investment and drive a top-down focus on changing the behaviours and culture throughout the organisation regarding these issues.

Read the full article **here.**

7. Cybersecurity innovations for the future

Today, the ever-evolving threat landscape, and increasing compliance requirements and security risks are driving greater levels of cybersecurity innovation. More businesses are seeking to implement emerging solutions to bolster their cyber-resilience.

NTT is leading this effort by developing cybersecurity innovations such as:

- **botnet monitoring and global backbone visibility**
- **its Cyber Threat Sensor, which provides location-agnostic, holistic, software-defined threat detection**
- **San-Shi, which enables the calculation and analysis of data, such as statics, from multiple sources without the disclosure of any confidential information, by using end-to-end encryption technologies**

Keeping an eye on and investing in cybersecurity innovations will ensure that you remain agile and that your business is geared to adapt to the ever-evolving threat landscape. But bear in mind that you'll need to adapt, and change your mindset: security must be embedded into the business' strategy upfront, not as an afterthought.

Read the full article **here.**

Most mature but most at risk

Globally, sectors experienced some interesting shifts in attack during 2018 – while cybersecurity posture isn't always aligned to risk.

Cyberpreparedness

The practice of ensuring that an organisation has developed, tested, and validated their capability to protect against, prevent, mitigate, respond to, and recover from a significant cyberincident, such as one that results in physical consequences to critical infrastructure.

Business leaders are prioritising cybersecurity as a boardroom issue and making strategic investments to boost their security profile. However, overall, current ambitions outpace cyberpreparedness.

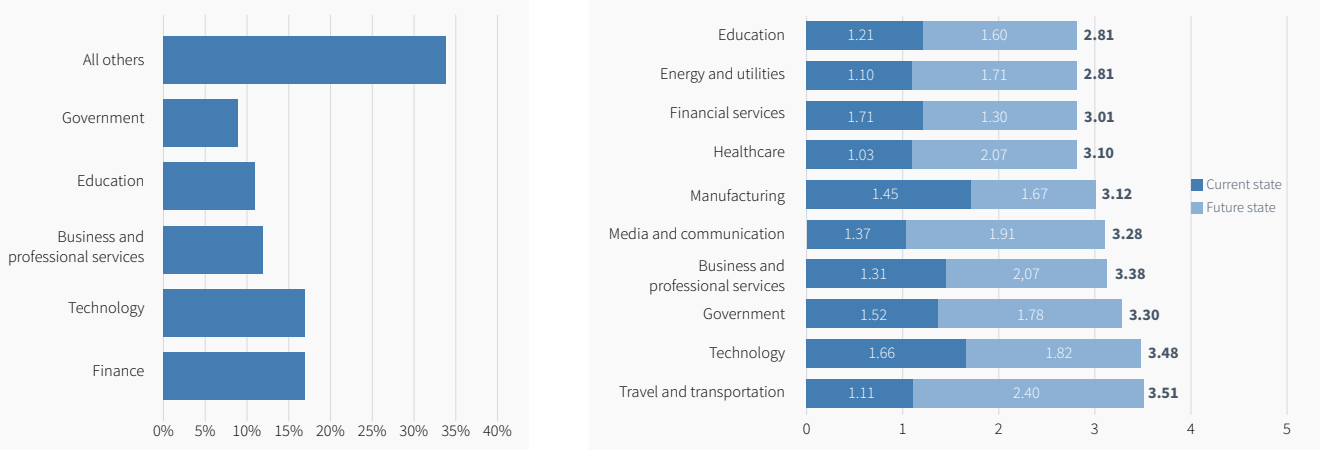
- Overall, cybersecurity maturity is generally lacking. The current global benchmark across all sectors is 1.45 out of 5.
- Interestingly, increased attack volumes correlate with an organisation's willingness to make strategic investments to improve their cybersecurity defences.
- And, ambitions significantly outpace preparedness, which means there's much work to be done to drive a robust security posture, in many sectors.

17%

The finance and the technology sectors are the most cybermature, however they were the most attacked, each representing **17%** of all attacks, and feature in the top five risks for every region.

Let's take a closer look at the best performers:

Figure 1: Global attacks by sector versus current and desired cybersecurity maturity levels



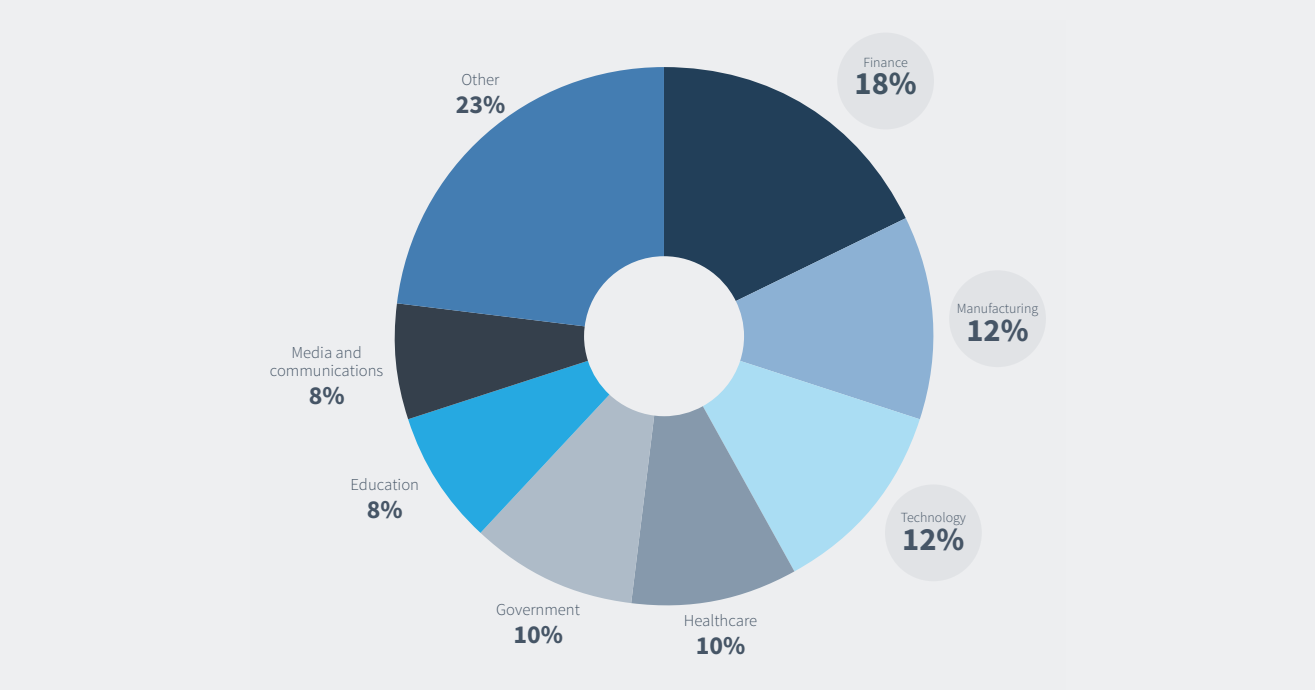
Maturity scale	Non-existent 0.00–0.99	Initial 1.00–1.99	Repeatable 2.00–2.99	Defined 3.00–3.99	Managed 4.00–4.99	Optimised 5.00–5.99
Process	No process exists	Ad-hoc and informal	Some basic templates or checklists exist	Formally documented processes are consistent	Formal and integrated workflows	Mature and automated workflows
Metrics	No metric exists	Ad-hoc reporting	Basic metrics, informal reporting	Formally documented metrics, manual reporting	Advanced metrics and semi-automated reporting	Fully automated reporting
Tools	No technology control exists	Planning underway	Basic functionality implemented with only elemental capabilities	Functionality implemented and aligned to policies	Integrated logging, manual correlation	Integrated platform, automated correlation

Organisations are seeking strategic relationships with partners to help guide digital transformation initiatives

Figure 2 below indicates the level of engagement that we've observed by organisations across various sectors, who're seeking assistance in building long-term security strategies and next-generation architectures.

- **Finance is more prepared to engage trusted partners** to advise on security roadmaps.
- **Technology and manufacturing sectors are** also **seeking assistance** to evolve their strategies and architectures.
- Finance and technology sectors were the most targeted during 2018 and are therefore responding by building a more robust security programme.
- Although **business and professional services** appeared in the top five most-targeted sectors, it **didn't engage strategically** to enhance its security profile. This places the sector at greater risk as its security posture may lack the resilience required to handle modern threats.

Figure 2: Cybersecurity Advisory engagements by sector



Finance

Finance has a current maturity state of **1.71** ahead of the global average across all sectors of **1.45.** However, there's still significant effort required if this sector is to achieve its future maturity ambitions of **3.01.**

An ever-expanding digital footprint, coupled with the value of sensitive data, credit card information, and other personally identifiable information held by this sector continues – and will continue – to motivate cybercriminals to set their sights on it.

Financial services businesses must therefore remain vigilant, due to the relentless nature of attacks and the continual emergence of more sophisticated types of malware.

Technology

The technology sector's current maturity level comes in at **1.66** – well behind the sector's average future maturity state of **3.48.** That said, technology organisations are generally willing to accept more risk than others, in pursuit of rapid innovation and collaborative environments to capitalise on new business opportunities to be gained by having first-mover market advantage.

However, organisations in this sector shouldn't let down their guard: they represent a rich source of valuable – and highly-marketable – intellectual property, which can be readily monetised in underground criminal forums, should adversaries successfully breach their defences.

24% Some 24% of organisations cite a lack of understanding of their current risk profile as a barrier to deploying better security systems.[1]

In contrast, let's swing our attention to one of the new global top five attack targets:

Education

Long-term malicious activity with continuous brute-force attacks on this sector, and a surprising increase in cryptojacking, have resulted in its unenviable inclusion in the top five this year.

However, globally education shows a marked lack of maturity with a current state of **1.21**, well below the global average of **1.45.**

Traditionally, this sector tends to prioritise student and research access, favouring open collaborative environments over rigid security controls that may impede productivity – hence a relatively low future maturity state of **2.81.**

We believe that greater vigilance is required in the year ahead.

Attack types defined:

Web attacks:

Attacks against services and applications that support a web presence, such as command injection, SQL injection, and cross-site scripting.

Reconnaissance:

Activity related to an attacker identifying systems and services that may be valuable targets.

Brute-force attacks:

The systematic use of username and password combinations to guess and identify credentials, to access a system or resource.

Service-specific attacks:

Attacks directed at services which often don't require authentication; they're most frequently observed in exploit attempts against common services, but often target databases and remote access services.

Cryptojacking:

Also known as coin mining, cryptomining, and cryptocurrency mining, cryptojacking is the illicit use of hijacked systems and CPU resources by cybercriminals to mine cryptocurrencies to generate revenue.

Credential theft:

Attacks targeting the theft of username and password credentials; cybercriminals' tactics include phishing, malware, and social engineering.

It's also important to note that cybersecurity maturity (and ambitions) **will always vary by sector.** Not all organisations do – or necessarily should – aspire to have the same levels of cybersecurity maturity.

Factors that will influence investment decisions include:

- regulations and legislation
- business strategy and alignment
- risk appetite
- threat profile
- industry
- competition
- culture

[1] Dimension Data's 2019 Global Customer Experience Benchmarking Report

Regional snapshot

35%

Globally, **35%** of all attacks originated from IP addresses within the **US and China, indicating that** these economic global powerhouses' infrastructure is being used as a launchpad for attacks.

The remaining attack sources varied across regions, with **EMEA and APAC** each experiencing a significant amount of attacks from within their own region.

Figure 3: Attack source countries by region

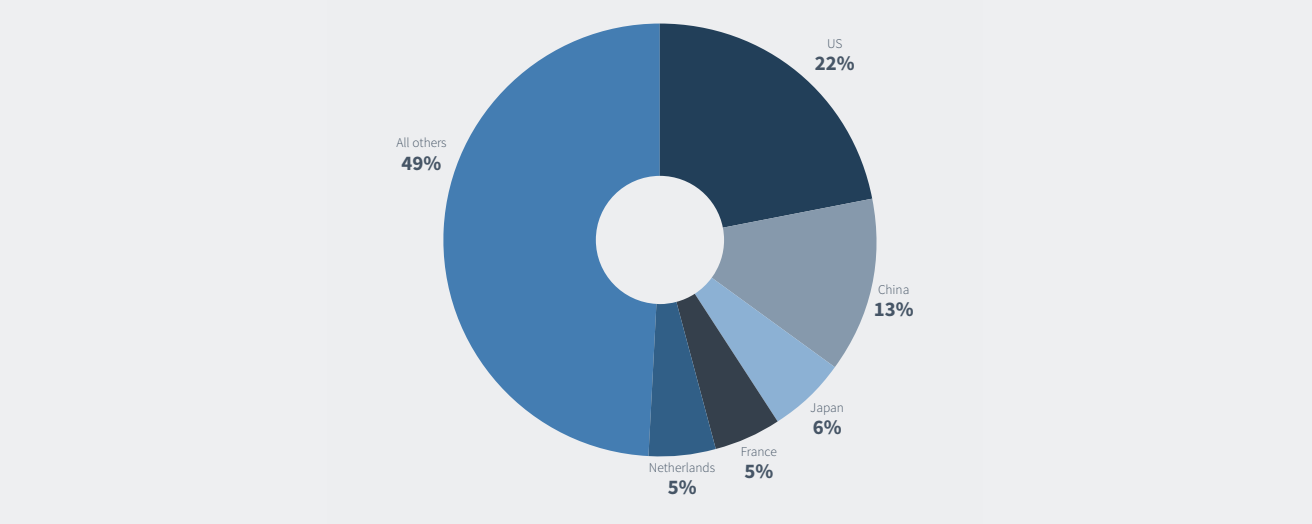


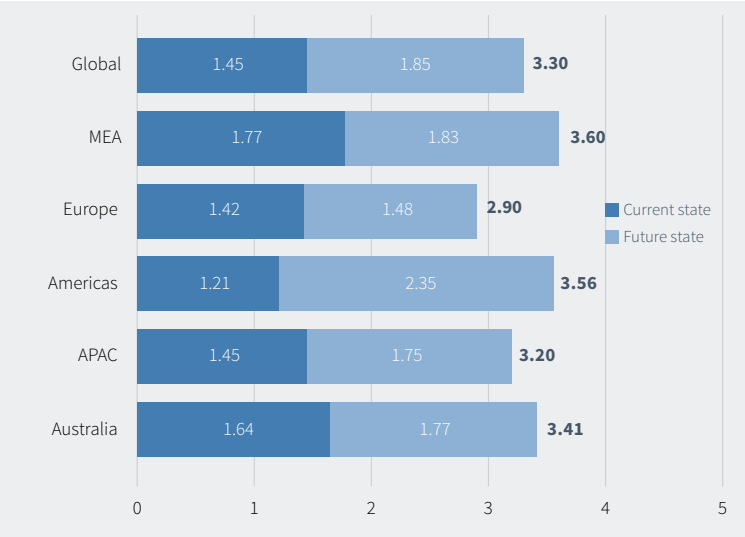
Figure 4: Regions' current and future cybermaturity states

Global

Overall, there's a **significant gap between regions' current state of cybermaturity versus where they want to be** over the next 12–36 months.

Ambitions outpace preparedness **most noticeably in the Americas and Europe,** both of which **fall behind the global benchmark.**

In terms of **future cybersecurity maturity ambitions** MEA rates highest, slightly ahead of the Americas.



Maturity scale

Non-existent	Initial	Repeatable	Defined	Managed	Optimised
0.00–0.99	1.00–1.99	2.00–2.99	3.00–3.99	4.00–4.99	5.00–5.99

EMEA

How prepared is EMEA?

Overall, Europe lags the global benchmark in terms of both current and future maturity posture.

MEA's maturity currently exceeds the global average but it's still far from its envisioned state.

The financial sector's current cybersecurity maturity level in Europe (1.21) falls well below the global average of 1.45. Given that this region experiences the highest volume of attacks against the financial services industry globally, this is concerning. This sector needs **increased vigilance** in the year ahead.

2.21

The MEA financial sector is currently **better prepared** to deal with attacks, with a current maturity level of 2.21.

The technology sector in EMEA has the most mature cybersecurity posture of all regions. Current maturity levels stand at 1.96 and 2.19 for MEA and Europe, respectively.

IoT

The manufacturing sector, although experiencing a decline in attacks, appears least ready or mature to handle any uptick in attack sophistication, especially in Europe. This raises concerns, given that organisations in this industry are undergoing rapid digital transformation. The automation of almost all business processes, the Internet of Things (IoT) deployments, and the increasing connectedness of the entire value chain, create agility but also raise cybersecurity risks and threat levels.

Americas

How prepared is the Americas?

Currently, the **Americas falls** short of the global maturity benchmark (1.45), rendering it least prepared to handle threats. However, its **future envisioned state exceeds the global benchmark.**

- Improved security preparedness in the finance sector has resulted in a decline in attack volumes, as threat actors seek out easier targets, especially those with weaknesses in their supply chains.
- Finance has a relatively mature cybermaturity posture in the Americas. The sector's current maturity state (1.71) is above the global average (1.45). It also has strong cybermaturity ambitions (4.08) compared to the average (3.3).

1.35

The technology sector's maturity rating (1.35) lags the global maturity average (1.45), despite it being the most-targeted sector.

- It's important to bear in mind that the technology industry is **generally prepared to take more risk** than other sectors, in pursuit of its aim to be first to market with innovative products. The US is specifically **renowned for its technological innovation.** Accordingly, its cybersecurity maturity is lower than the global average. However, this is something that could make it less sustainable in the longer term, should a breach be discovered.
- The healthcare sector in the Americas is **better prepared** than several other regions. Nevertheless, its **current maturity is lacking (1.32)** and still trails the global benchmark despite the rising number of attacks being launched against this sector.
- The education sector in the Americas (as in all regions) is **least prepared** to handle the increased sophistication of cyberthreats. This is concerning given the rise in the percentage of attacks on the education sector from 1% to 7%, between 2017 and 2018.
- Education can expect to be **more targeted and less prepared** to handle attacks, unless swift and decisive action is taken.

APAC

How prepared is APAC?

APAC's cybersecurity maturity is close to the global benchmark and it's doing well when compared to some other regions, such as the Americas.

The technology sector's cybersecurity maturity (1.69) is above the global average (1.45) but it's facing increasing levels of interest on the part of cybercriminals.

0.94

The **APAC education sector's maturity is weak** despite a constant barrage of attacks, which places it at greater risk. Its current cybermaturity level stands at just **0.94,** significantly trailing the global benchmark of **1.45.**

1.88

The finance sector has experienced a decline in attacks over the last year. We believe this is partially due to their current maturity of 1.88, which **stands ahead of the global average,** and not far behind Australia and MEA. The sector also has a mature security posture compared to the most-targeted sectors in the region (technology and education).

Finance will be better prepared to deal with any uptick in attacks on their sector in the year ahead. In addition, its high levels of preparedness to handle threats may well motivate cybercriminals to shift their focus towards less-mature sectors.

Australia

How prepared is Australia?

Australia remains consistently above the global average benchmark of 1.45 across all measured capabilities.

- The **finance sector in Australia outperforms most other regions and far exceeds the global average benchmark.** This leaves it **better prepared** to tackle increased focus from cybercriminals.

2.13

The finance sector's **cybersecurity maturity (2.13**) makes it the second-most mature region behind MEA (2.21).

26%

The region is one of the **most adequately prepared** to handle a **surge in threat volumes and sophistication against finance,** which rose from 13% of all attacks in Australia in 2017 to 26% in 2018.

- The **government sector** in Australia is currently the **most-prepared region to defend against attacks (2.92)** and it **demonstrates leading security vision and strategy.**
- Not only does the region demonstrate strong existing cybermaturity in the government sector, it also has **very strong ambitions** – with a desired future state of almost 4/5.
- We believe that **new compliance regulations in the region** as well as strong leadership in this sector, contributed to these relatively positive results.

1.92

The education sector's current **cybermaturity (1.92) is higher than in other regions,** which leaves it better placed to deal with cyberthreats.

- **Attacks on the education sector declined** due to relative increases in cybersecurity maturity in this region and accounted for the sector **dropping out of the top spot** of most-targeted sectors.

Four types of hostile activity dominate global cyberattacks

New vulnerabilities on the rise

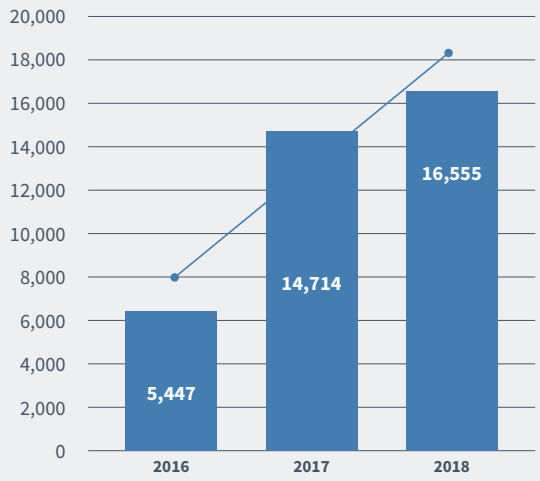
12.5%

Vulnerabilities are increasing at an alarming rate. Overall, we saw a **12.5% growth in vulnerabilities discovered, compared to 2017.**

In fact, **2018 set a record for the number of new vulnerabilities identified and reported in a single year**[2]. These vulnerabilities are subsequently being 'weaponised' for use in adversarial campaigns and automated toolsets.

According to recent research[3] undertaken by Dimension Data, respondents perceive 'application and operating system vulnerabilities' as one of the top four threats affecting business.

Figure 5: Growth in vulnerabilities



Many vulnerabilities were **discovered in older software and have been present for years.** For instance, the GNU Bash vulnerability (also known as 'Shellshock') which was discovered in 2014 and affects most Unix, Linux, and Mac OS X platforms, continues to be one of the most commonly targeted vulnerabilities today. Some vulnerabilities were in **processor chips** and have the potential to shake up the entire computing world.

Other, new, vulnerabilities this year were **introduced through patches originally intended to resolve other vulnerabilities.**

The increase in vulnerabilities over the past two years is a significant challenge to organisations. That's because many of these vulnerabilities exist in **common systems, utilities and applications, and application code libraries used to support daily operations.**

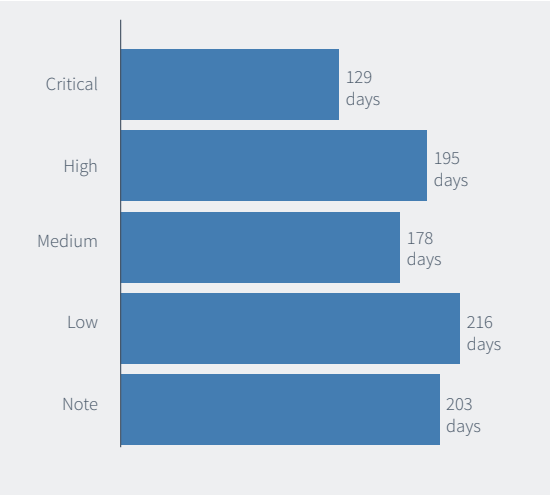
Figure 6 overleaf, drawn from recent research undertaken by WhiteHat Security[4], indicates that prioritisation remains a challenge with development teams not prioritising high-risk vulnerabilities when it comes to static application security testing (SAST). Dynamic application security testing (DAST) remediation prioritisation reflects the seriousness of the vulnerabilities. Overall, the research revealed that:

- Organisations' remediation strategies are failing.
- **Time-to-fix has increased** for all risk levels except for 'medium' risks.
- The **window of exposure** across all industries remains the same: **too long.**

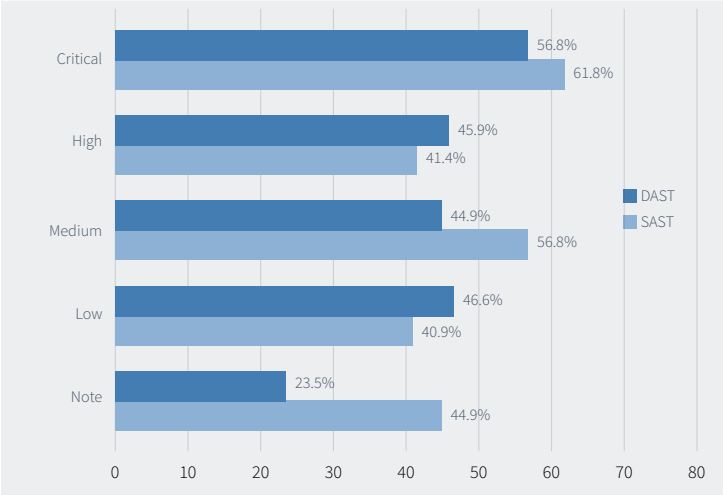
[2] CVE Details, 2018
[3] Dimension Data's 2019 Global Customer Experience Benchmarking Report
[4] WhiteHat Security 2018 Application Security Statistics Report, Volume 13: The Evolution of the Secure Software Lifecycle.

Figure 6: Remediation and time-to-fix levels

Time-to-fix by risk level



Remediation rates by risk level



Four types of hostile activity dominate global cyberattacks

73%

Some 73% of all hostile activity falls into four categories: **web attacks, reconnaissance, service-specific attacks, and brute-force attacks.**

Web attacks:

Web attacks doubled and became the **top type of hostile activity,** partially due to the number of vulnerabilities found in common applications. They now account for **over 32% of all hostile traffic** – that means nearly a third of all hostile activity is now directed against organisations' external web presence.

Reconnaissance:

Reconnaissance represented **16%** of all hostile activity. It's often an indicator of a pending attack against an organisation, but isn't immediately damaging.

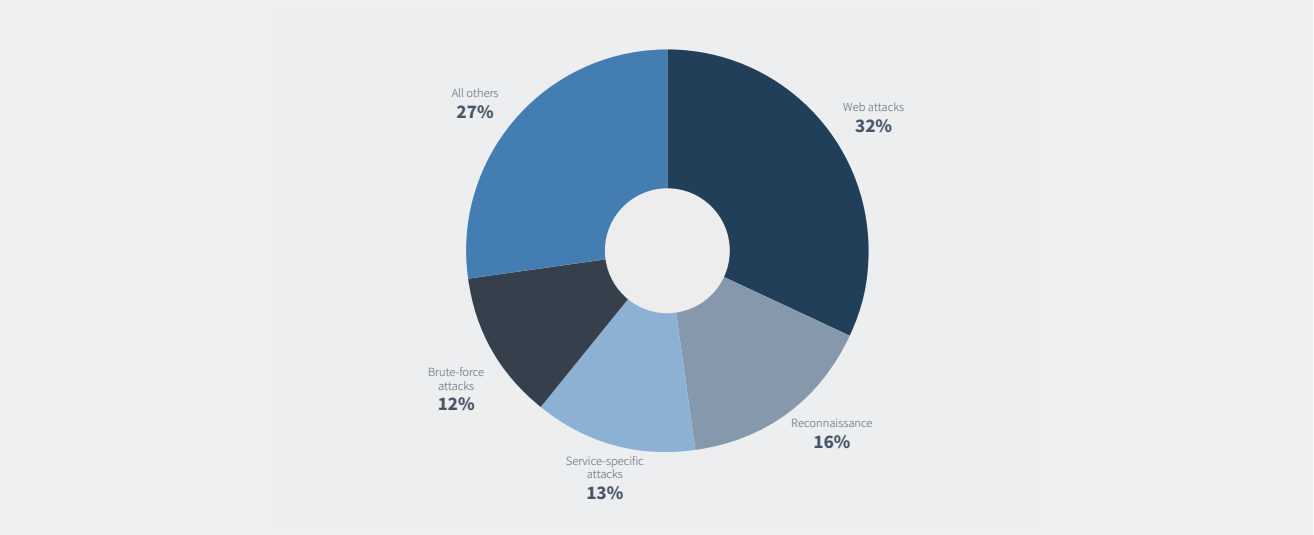
Service-specific attacks:

Service-specific attacks accounted for **13%** of all attacks globally and ranked as the third most common type of hostile activity.

Brute-force attacks:

Brute-force attacks continue to be a popular attack mechanism, representing nearly **12%** of hostile traffic globally and were primarily directed at education and retail targets.

Figure 7: Global hostile activity



Attacks targeting Bash, Apache Struts, and Samba accounted for 54% of all hostile activity.

Cryptojacking:

Cryptojacking, while still in its infancy, caught many organisations off-guard and represented a significant amount of hostile activity – at times **accounting for more detections than all other malware combined.** According to a recent joint paper[5] by the Cyber Threat Alliance (CTA), NTT Security, and other CTA members, cryptojacking detections **increased by a staggering 459% between 2017 and 2018.**

In fact, the growth of **cryptojacking** activity has had a similar effect to the impact of ransomware in 2016.

Credential theft:

Credential theft is up, with attackers now targeting cloud credentials as more applications and data move to the cloud, as a consequence of organisations' digital transformation journeys. The technology and education sectors were **caught off-guard specifically in this area.**

What is ...

- '**Shellshock'** is a set of vulnerabilities associated with the Unix 'Bash' shell, which could give an attacker control over the targeted system. It's notable because the bug had been present in application code for many years before it was discovered.
- **Apache Struts** is an open-source web application framework for developing Java web applications, which is widely used by enterprises worldwide, including many Fortune 100 companies. In August of 2018, researchers disclosed a critical remote code execution vulnerability in the Apache Struts web application framework that could allow remote attackers to run malicious code on affected servers.
- **Samba** is a suite of tools that provides cross-platform compatibility for file and print services between Unix and Microsoft Windows-based platforms.

[5] The Illicit Cryptocurrency Mining Threat, Cyber Threat Alliance, 2018

How to establish cyber-resilience and maturity

Defending your organisation is no easy task, but focusing on key areas can assist in developing an effective security strategy.

Cybersecurity requires strong leadership and business alignment to drive change

71%

It's now more important than ever to adapt a business-outcome driven approach to tackle cybersecurity and compliance challenges. Some 71% of organisations believe security is important to the organisation's digital strategy and ranked it important of all technologies.[6]

Cybersecurity is in a unique position as a key enabler for digital transformation, and a leading value driver to deliver competitive differentiation, enhancing client and employee trust, as well as increasing business reputation.

Gain executive buy-in – and ensure your people know that cybersecurity is everyone's responsibility. Culture shouldn't be considered as an afterthought.

According to our recent research[7], 64% of businesses view ineffective understanding of their current risk profile as one of the primary inhibitors to deploying better security controls. Coupled with a lack of alignment between business and security strategy, as well as an inability to articulate risk in business and financial terms, this can leave security on the back foot.

Adopting strategic cybersecurity advisory services that span the entire lifecycle from developing a strategy and plan aligned with business needs, optimising security controls, to designing next-generation security architecture, policies, and frameworks will drive focus and help to build the business case for cybersecurity investment.

Recommendations for upping your defences against common attack types

- **Cryptojacking:**
  - apply least privilege controls
  - implement egress and ingress filtering restrictions
  - implement browser plugins to limit site functionality (JavaScript)
  - deny Stratum protocol usage
  - segment network environments
- **Web application attacks:**
  - prioritise patching
  - segment your network environment
  - enforce secure coding practices
  - deploy application-aware firewalls
  - perform regular vulnerability scanning
- **Credential theft:**
  - implement multi-factor authentication
  - segment the network environment
  - enforce 'least privilege' and segregation of duties
  - implement network activity monitoring and data loss prevention
  - educate employees to be vigilant about phishing attacks

[6] Dimension Data's 2018 Digital Means Business Benchmarking Report
[7] Dimension Data's 2019 Global Customer Experience Benchmarking Report

As the digital world becomes more interconnected, build a holistic and integrated security ecosystem

Today, cybersecurity leaders' jobs are made more difficult as the number of areas and 'things' that need to be secured is constantly increasing. Your infrastructure is no longer just physical, it's cloud, and hybrid too. As you adopt the Internet of Things, and the cloud, there are many new kinds of devices and connections to secure. Your users, whether employees or customers, are connecting through various different networks. You must also secure interactions with your partners and others in your supply chain.

The cybersecurity skills gap only exacerbates the security implications inherent in digital transformation. Rather than devoting extensive resources to build out your own in-house security operations centres and extended security teams, engage with a trusted partner to deliver these capabilities as a managed security service. Outsourcing these capabilities benefits the business by providing diversified talent pools, in-depth expertise, innovative technologies, and proven processes to drive business outcomes with reduced upfront capex.

Keep up to speed with and embed compliance requirements into your strategy

Data security, protection, and privacy has been a hot topic for the last few years. Today there's no shortage of tools for information-sharing and collaboration. As maturity in these areas continues to evolve, it's vital to keep pace with regulatory requirements. Governance, risk, and compliance should be part of the board and management agenda, not simply an activity delayed until an audit is looming.

Success is achieved when you've invested proportionately in people, processes, and tools to provide a solid foundation of security and data privacy expertise embedded into the overall strategy, across all technology stacks. Benchmarking your organisation against industry best practices and control frameworks provides an easy way to measure the return on your security investment. Simply put, you cannot manage what you cannot measure. Understand your compliance posture and plan ahead so you can achieve your security ambitions.

Embrace innovative products and solutions

Legacy methods and tools are still relatively effective at providing a foundation for consistent mitigation, as most attacks can be prevented with basic security controls. Defence-in-depth strategies, coupled with security-by-design methodologies, will reduce your attack surface and enhance cyber-resilience. But adversary tactics change – and new attack techniques will be developed. This requires an innovative approach to security that enables the business to remain flexible and agile.

In response, embrace automation to allow you to accelerate your efforts at the speed of digital business and integrate cybersecurity within your DevOps practices. As you apply DevOps to your application development, every incremental release must be secured seamlessly in both your development and production environments. Organisations who embed security testing within the software development lifecycle achieve significantly better application security outcomes than those who don't. Also, consider how improvements in machine learning, when applied to cybersecurity, could work in your favour.

> Reducing the need for human involvement in processes and tasks is seen as the main impact artificial intelligence will have on mitigating cybersecurity risks. Over 38% of organisations expect to see benefits through enhanced threat detection capability, while more than 37% expect improvements to be realised through accelerated incident response.[8]

Likewise, embedding **security automation** into threat detection and incident response processes will optimise the effectiveness of your controls, enabling your security teams to focus on higher-value activities. **Cloud-native and cloud-enabled security** controls may also bring about efficiencies and cost savings, enabling better protection for mobile users, regardless of their location and the devices they're using to access your organisation's infrastructure.

[8] Dimension Data's 2019 Global Customer Experience Benchmarking Report

Supporting technologies that can help bolster your cyberdefences:

- identity and access management
- multi-factor authentication
- vulnerability management
- next-generation firewalls
- web application firewalls
- web and email security
- data encryption
- data loss prevention (DLP)
- cloud access security brokers (CASB)
- cloud workload protection
- endpoint protection platforms
- application security testing
- SIEM
- threat intelligence
- security orchestration and automated response

Embrace predictive and proactive intelligence capabilities

Predictive, intelligence-driven processes and technology will expand your coverage, visibility, and enhance your ability to proactively respond to cyberevents.

Define a plan for regular assessments, both technical and non-technical.

Technical assessments help identify and reduce your risk exposure. Include not only traditional penetration testing activities, but also application testing and social engineering. Leverage threat intelligence to shift from a reactive stance to one that incorporates active cyberdefences to swiftly identify, track, and mitigate threats in a predictive manner.

Analysis methodology and resource information

Data sources, analysis, and reporting

10,000

With visibility into a vast portion of the world's Internet traffic, 10 Security Operations Centres and seven research and development centres, collectively, NTT Security, Dimension Data, and NTT's operating companies continuously gather cybersecurity data from 10,000 security clients on six continents.

The Executive Guide to the NTT Security 2019 Global Threat Intelligence Report contains data gathered from 1 October 2017 to 31 September 2018. The analysis is based on client information, including:

- log, event, attack, incident, and vulnerability data; incident response engagements; threat intelligence; and other research sources
- benchmarks from our Cybersecurity Advisory client engagements

This year, we detected a total of **150+ million attacks** and analysed **6.1+ trillion logs.**

Our Cybersecurity Advisory is a business-outcome driven consulting engagement that uses empirical evidence and benchmarking to make practical recommendations. The service:

- establishes current maturity levels, and identifies gaps in existing security architecture and security management practices
- provides recommendations on how to reduce operating costs and improve efficiencies and better meet compliance and regulatory obligations
- assists with informed decisions regarding immediate and strategic security priorities

Global Threat Intelligence Centre (GTIC)

The NTT Security Global Threat Intelligence Centre protects and provides clients with services and tools to prevent and provide early warning notifications of risks and threats, 24/7, encompassing:

- threat research and management
- vulnerability research
- detective technologies development
- communication with clients

The GTIC takes its threat and vulnerability research and combines it with its detective technologies development to produce applied threat intelligence.

About Dimension Data Security

Dimension Data keeps your business safe, secure, and compliant with a new generation of cybersecurity fit for the digital world. We help you create a digital business that's secure by design and simplifies the cybersecurity experience across your organisation as you innovate, and transform your business.

With our threat intelligence insights, you're better prepared to detect and respond to cyberthreats while managing risk. We help you to avoid downtime and build an agile and predictive security ecosystem that spans your users, applications, and infrastructure.

These efforts are generally led by cybersecurity consulting services – including our Cybersecurity Advisory – which give you the strategies, architectures, and management processes to enable you to achieve your business goals.

Many of our clients opt to consume these capabilities as Managed Security Services – delivered from NTT Security's global Managed Security Service Platform – which give them security intelligence, analytics, and automation as a managed service. And our technical and support services provide the expertise and resources needed to help you design, deploy, resource, and support your ICT environment.

> Over 15% of businesses cite a lack of dedicated cybersecurity personnel as a barrier to deploying better security systems.[9]

Our credentials include:

- over 2,000 security specialists, architects, and engineers certified to the highest levels across multiple vendors, technologies, and industry standards
- vast experience in managing and optimising security infrastructure for clients in every industry, across the globe
- over 15,000 security engagements in approximately 47 countries, over the last 15 years
- billions of attacks analysed to inform our depth of insights
- direct access to an ecosystem of leading partners means we can select the technologies you need and pre-integrate them at the application programming interface level, to give you the best security products available

About Dimension Data

Dimension Data Dimension Data is a global systems integrator and managed services provider for hybrid IT. Headquartered in Johannesburg, Dimension Data employs over 28,000 people across 47 countries. We bring together the world's best technology provided by market leaders and niche innovators, providing clients with the service support that they need for their business, from consulting, technical, and support services to a fully managed service. Dimension Data's cybersecurity practice helps clients to envision and build digital businesses that are secure by design. Together with NTT Security, we have more than 2,000 experts across 47 countries to support clients on a secure digital transformation journey.

As a proud member of the NTT family, our continued investment in innovation enables us to find new ways to deliver services to clients today, while also keeping an eye on the future.

Visit us at https://www.dimensiondata.com/ to learn more.

NTT Group resources

NTT Security
nttsecurity.com

Dimension Data
dimensiondata.com

NTT DATA
nttdataservices.com

NTT Communications
ntt.com

NTT-CERT
ntt-cert.org.

NTT Innovation Institute
ntti3.com

To learn more about how we can help to protect your digital business, visit our cybersecurity expertise page.

For contact details in your region please visit https://www.dimensiondata.com/en/contact-us

[9] Dimension Data's 2019 Global Customer Experience Benchmarking Report