# CODES TO RESILIENCE

Cyber Resilience in
Travel & Tourism

WORLD
TRAVEL &
TOURISM
COUNCIL

Microsoft
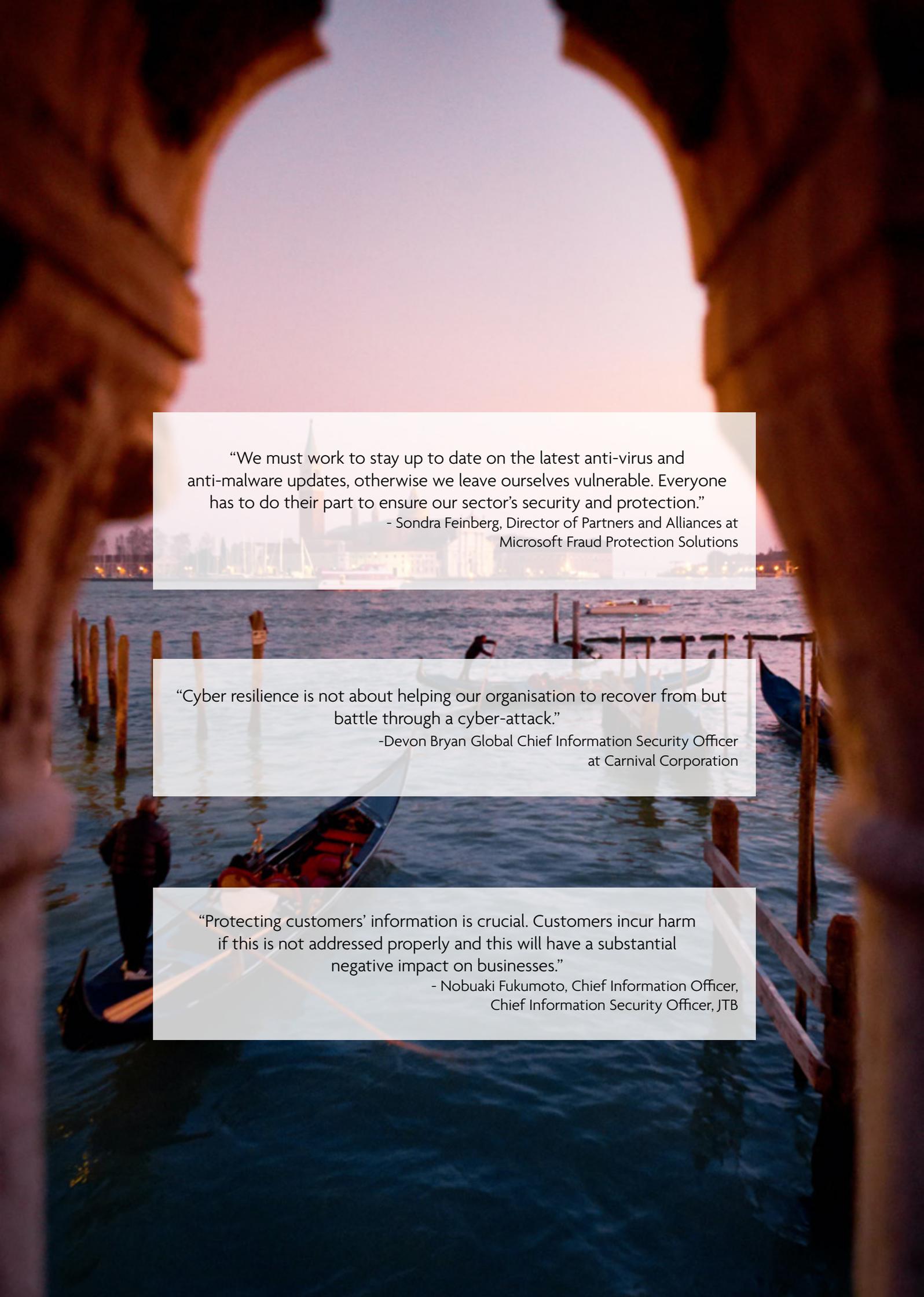
"We must work to stay up to date on the latest anti-virus and anti-malware updates, otherwise we leave ourselves vulnerable. Everyone has to do their part to ensure our sector's security and protection."
- Sondra Feinberg, Director of Partners and Alliances at Microsoft Fraud Protection Solutions

"Cyber resilience is not about helping our organisation to recover from but battle through a cyber-attack."
-Devon Bryan Global Chief Information Security Officer at Carnival Corporation

"Protecting customers' information is crucial. Customers incur harm if this is not addressed properly and this will have a substantial negative impact on businesses."
- Nobuaki Fukumoto, Chief Information Officer, Chief Information Security Officer, JTB

INTRODUCTION

The outbreak of COVID-19 propelled the world into a more digital future, enabling life and business to continue as much as possible whilst protecting public health. However, with the many opportunities for growth and innovation that digitisation creates, new challenges emerge, specifically as they relate to cybercrime.

Over the past decades, digital technologies have become an integral part of high functioning businesses with very few organisations able to operate without some sort of digital presence or intervention. In effect, for most businesses a high level of engagement with cyber systems is necessary to enable them to operate. This doesn't just include information technology (IT) but also operational technology (OT) used to manage equipment and buildings.

In an increasingly digital world, cyber security is as important as the digital innovation it protects. Innovative systems that simplify processes and improve customer and employee experiences facilitate good business operations. These systems hold significant amounts of information about people, businesses, and even governments Hosting this information, which can be both sensitive and confidential, and managing its movement is essential. In today's networked and interconnected world, information is often transferred between systems, resulting in the expansion of the risk area, whilst further highlighting the importance of secure systems.

In this context, WTTC and Microsoft hope that this joint report can serve as tool for the Travel & Tourism sector to better understand how cyber resilience is shaping the sector and plan for a safer and more resilient future. The report, which is built on desk research and in-depth interviews with cyber security experts in leading Travel & Tourism organisations, is divided into three sections namely-

> **cyber resilience in context**
>
> **key issues**
>
> **seven good practices**

The first section explores cyber resilience in the context of Travel & Tourism while the second section addresses key issues, highlighting their importance and why they remain priorities for the future. The final section outlines the pillars of effective and resilient cyber systems to help strengthen cyber resilience and maintain business continuity based on the lessons learnt prior to and during the pandemic.

As a sector that supported 334 million jobs in 2019 and continues to connect people across the world, it is essential that Travel & Tourism is resilient both online, as people connect digitally, and offline. Digitisation has enabled the sector to enhance its offering to consumers and its opportunities for employees however, it has also introduced new risks. These risks pose tremendous financial, operational, and reputational threats to the sector requiring they be proactively identified and addressed to ensure the long-term resilience of Travel & Tourism.

CYBER RESILIENCE IN CONTEXT

For Travel & Tourism organisations that operate across borders, digitisation has become a strong enabler of business. For years, the sector has increasingly incorporated digital technologies and made the necessary investments to support this growth. This enabled the sector to expand its reach leading to Travel & Tourism contributing 10.4% to global GDP and creating one in four of all new jobs on the planet in 2019. It is a key driver of job creation and prosperity.

IMPACTING BUSINESSES LARGE AND SMALL

While cyberattacks on large enterprises are well-reported and attract headlines, these organisations are not the only targets of cyber criminals. Research suggests that small to medium-sized enterprises are also vulnerable and, in some cases, cyberattacks may lead a business to shut down. In England, for instance, 43% of all cyberattacks are targeted at small businesses[1] and in the United Kingdom, the United States, and Europe 72% percent of Small to Medium Enterprises (SMEs) reported experiencing at least one cyberattack[2]. In effect, 77% of respondents noted lack of qualified personnel as the biggest obstacle in mitigating cyber risk, followed by budget and an understanding of how to protect against cyberattacks. In fact, 60% of SMEs fail within six months of falling victim to a cyberattack[3]. With approximately 80% of all Travel & Tourism businesses being SMEs, mitigating cyber risk must remain a priority for the sector.

Technology is involved in almost every aspect of the Travel & Tourism experience – from inspiring travellers, booking, and paying for a holiday to flying a plane and embarking on a cruise.

Given that these experiences can be booked in one region and enjoyed in another, the role of legislation around individual data protection and organisational cyber security is immense.

It dictates what can be done and how it must be done, making compliance a key part of the digitisation process.

EXPLOITING VULNERABILITIES

Cyber criminals tend to be opportunistic and will exploit any possible area of vulnerability, from a payment process to a loyalty programme. While loyalty programmes enhance the travel experience by creating reward opportunities based on travel, they are also a target of cyber criminals. These programmes contain sensitive data which makes them susceptible to attack, underlining the need to treat these programmes as part of the larger eco-system of the business. Devon Bryan at Carnival Corporation highlighted that Carnival "has layered defences that get activated to secure our sensitive systems and data; these are supported by ongoing monitoring. So, the loyalty programme receives the same protection we give other highly sensitive data".

THE FINANCIAL COST OF CYBERCRIME

The Travel & Tourism sector is diverse with industries including hospitality, cruise, aviation, OTA, and technology, among others. Regardless of industry, if information is stored in the cybersphere it is vulnerable to an attack. In 2019, the average number of cyber breaches across sectors grew by 11% and the average cost of cybercrime for an organisation was valued at US$13 million[4]. With a 67% increase in security breaches between 2015 and 2019, the threat of cybercrime is imminent for any business.

Indeed, while travel-related risk varies across regions, data-related risk is not confined by borders. In 2018 almost 514 hotel data records were stolen and lost worldwide[5]. What's more, according to the European Aviation Safety Agency (EASA), there were 1 000 cyberattacks each month on aviation systems in 2016[6]. The International Air Transport Association (IATA) estimated airline payment fraud was valued at a minimum of US$1 billion in 2020[7] and a 2011 report by the UK government found IP theft in Travel & Tourism cost businesses in the sector £200m annually[8].

67%
increase in security breaches between 2015 and 2019

11%
growth in the average number of cyber breaches across sectors in 2019

Average cost of cybercrime for an organisation was valued at

US$13 million[4]

IBM found that 2021 had the highest average cost of data breaches in 17 years[9]. Indeed, the financial cost of cybercrime has continued to rise in the last two decades, making it a growing risk that requires immediate and increased attention.

THE REPUTATIONAL COST

Despite the devastating impact of COVID-19 people's desire to travel has been unwavering, with the overall reputation of the sector remaining positive. According to Kelly White at Mastercard, "most people assume and expect security and privacy", both in how the data is being used and stored. This highlights the trust consumers have had in their providers, even in the absence of overt safety measures. Yet, it comes with the responsibility to keep that data and information secure. As highlighted by Nobuaki Fukumoto at JTB, "protecting customers' personal information is crucial. Customers incur harm if this is not addressed properly, and this will have a substantial negative impact on businesses."

In 2018 there were 7 billion Internet of Things (IoT) devices, objects that are connected to and interface with the internet and/or each other, with more than triple (26.6 billion) being active in 2019. What is more, it is estimated that more than 75 billion IoT devices will be connected to the web by 2025[10] and cybercrime is estimated to grow by 15% year on year to cost the world US$10.5 trillion annually by 2025[11]. Indeed, cyber resilience is foundational to effective business and risk management and cyber resilience is fundamental to the resilience of the Travel & Tourism sector.

KEY ISSUES

To better understand and enhance cyber resilience within Travel & Tourism, four key issues form the lens through which this report examines areas of cyber vulnerability and challenges ahead. While these issues will vary for each organisation and area of operation, addressing each improves cyber protection and enhances resilience.

SECURING IDENTITIES

Identity data supports travel providers in collecting revenue while boosting efficiency and personalisation. With the rise in new technologies and the increased sharing of personal information, including through the use of biometric authentication and other contactless technologies, the need to further secure this information has accelerated. As the ability to confirm identity has diversified, opportunities for criminals to access this information in various ways and compromise multiple systems has also accelerated. The World Economic Forum found that identity theft is the second highest cyberattack method global cyber leaders are most concerned about[12] and with good reason.

Dan Johnson at Mastercard describes identity data theft as "building the history of a person to assume their identity." Indeed, access to personal information enables criminals to harm a victim in many ways. For instance, access to home addresses is a lucrative threat area that could be leveraged for further financial gain particularly when homeowners are travelling and away from their homes. What is more, with access to identity data, cyber criminals could create accounts in the victim's name and exponentially increase the scale of their attacks.

With **access to identity information** also becoming an important part of completing payment processes, such as confirming personal information about card holders, there is a need to reduce the amount of information shared, with providers continuing to find ways to confirm identity without revealing the underlying information. Multi-factor authentication systems are also an effective mitigation measure with two-factor authentication being the minimum requirement. This is especially relevant for loyalty programmes, as some may require customers to share information into a different ecosystem either by logging into a different website or contacting a separate provider.

Phishing, malware, and ransomware threats are constant, with ransomware responsible for 23% of cyberattacks in 2021 and phishing employed in 33% of cyberattacks[13]. While the software has been enhanced, the methods of attack remain similar as threat actors largely gain access to cyber environments through phishing, credential theft, or remote desktop control. Research found that 96% of phishing attacks arrive by email and, in 2020, 1 in every 4 200 emails was a phishing email[14]. As such, staff education and training is a key aspect of cyber security and resilience. Trained staff, who know how to avoid falling victim to attacks and what to report, can enhance security systems and decrease access to the cyber systems.

> "We are the first line of defence, so we must be trained properly in cyber security mitigation,"
> -Alain Simon at Amadeus, while emphasising the value of training all members of staff.

Indeed, **staff training** is critical to effective cyber security and resilience and this training should be tailored, with more in-depth training required for those with access to more sensitive data or larger amounts of data. What is more, access to data should be based on what the employee most needs. In many organisations, staff members are given access to data they do not need which unnecessarily exposes them and the organisation to attack. Anyone with access to the system can compromise it by falling victim to a phishing attack; insider threats are a growing concern. While a malicious insider is an employee who intentionally causes or enables a breach by compromising the security of the system, compromised and careless insiders cause or enable a breach unintentionally. Compromised insiders may have their computers infected with malware or their credentials compromised while careless insiders are unaware that they are exposing the system to threats.

OPERATING SECURE BUSINESSES

As business operations are enabled by the effective functioning and security of both IT and OT systems, the security of all connected IoT devices should remain a priority. Indeed, investment in cyber security has intensified with the support of internal experts and outsourcing to specialist businesses.

Through effective and regular training, organisations can decrease the number of insider threats as a result of negligence or ignorance.

"Cyber security, by design, is meant to introduce friction – and by doing so creates an opportunity for innovation to enable increasingly easier, more trusted experiences for end users," says Anudeep Parhar of Entrust.

Ultimately, the protection of identity information is paramount and securely and effectively using, protecting, and deleting that information is an essential part of cyber resilience.

Travel & Tourism organisations have a more complex environment than other sectors as many employees work across the globe and it is important to ensure that transportation systems are safe and secure whilst they are in motion and with limited connectivity. For example, cruise ships must be self-sufficient, providing all services and amenities to ensure an enjoyable experience for travellers whilst ensuring that they are safe. Greg Sullivan at Carnival Corporation explains, "our ships are floating cities so every solution you need for cities we have on ships. We carry all of the available risk that could exist in the world so if I have a device on a network, I have a potential vulnerability."

While the specific risks for cruise and other industries will differ, some common risks apply. One such risk is **access to the Wi-Fi network**. Free and fast Wi-Fi has become a key booking requirement for both leisure and business travellers with 85% of guests indicating that Wi-Fi quality affects their decision to rebook with a property or hotel brand[15]. However, over 90% of those same guests shared concerns about personal data security on that network. From the use of apps that may have been compromised to accessing emails with potential malware, free access to Wi-Fi requires a flexible security response that must be updated regularly.

Another common risk for the sector arises from the **integration of data** from different systems from a business acquisition, a different travel provider, or from a separate system such as a loyalty programme. This introduces concerns not only over aggregate risks but over data governance and privacy protection of customer and employee data. In the case of acquisition or partnership issues may arise due to differing cyber hygiene practices. Organisations may import ransomware or expose themselves to poor privacy practices. In the case of mergers or acquisitions, procedures are required to ensure the data is clean prior to importation, and that any systems that are connected meet the organisation's cyber security standards. According to Daniel Dobrygowski at the World Economic Forum, cooperation across cyber systems is key; he noted that "it can be difficult to have a cohesive approach to cybersecurity, but this challenge is solvable through cooperation."

Similarly, for **loyalty programmes**, consistent standards and protocols are required when working across different systems to ensure full protection of user information. Experts argue the best approach is for loyalty programmes to exist in the same ecosystem as the larger organisation, ensuring they are subject to the same protections on sensitive customer information. This also enhances the customer experience as they will not need to provide as much sensitive data when signing up for loyalty programmes. If applicable, loyalty programmes should receive additional, tailored solutions. Each aspect of the business has its own requirements; Deneen DeFiore McGarvey at United Airlines adds that "this starts with strong data protection and tuning specific protection requirements to additional dimensions".

The **hygiene practices** needed to mitigate risk and enhance cyber resilience begin with prioritising cyber resilience at the highest levels of the organisation and, subsequently, providing financial, technological, and human resources required to mitigate risk. While budget is a factor in mitigating risk, it is clear that for cyber resilience a multi-dimensional approach is required. According to Alain Simon at Amadeus, "the issue is not a problem of budget, but a problem with resources". In effect, threat levels and vulnerabilities must be identified and then the appropriate budget, software, and skillsets can be allocated to mitigate risk. Michael Jabbara at Visa further highlights this, noting

that "humans operate these machines and software, so it is vital we ensure that they have the right skillset." Simone Fortin of MSC Cruises agrees that the focus should be on identifying and mitigating risk; "the main challenge is about how we work together to identify the risk and address it promptly. You cannot put a price on security of livelihood and trust."

Keeping software up to date, protecting identities, and ensuring strong data governance are essential hygiene measures. Understanding how vulnerable systems are and ensuring that protections against known vulnerabilities form the foundation of good security practices. As Sondra Feinberg at Microsoft highlights, "we must work to stay up to date on the latest anti-virus and anti-malware updates, otherwise we leave ourselves vulnerable. Everyone has to do their part to ensure our sector's security and protection." These updates should be informed by the latest developments in cyber risk mapping and from active threat hunting in the local system. This can be done through tools and applications to identify gaps and vulnerabilities to better protect systems and the network.

> "Breaking cyber security systems to identify gaps and vulnerable points is effective".
> -Michael Lemberger at Visa

Indeed, regular and proactive system testing by skilled employees enhances cyber security and resilience. What is more, security should be visible because "security by obscurity is not a good tactic," according to Manon Gaudet at IATA.

With the entire supply chain being a potential area of entry for threat actors and criminals, proactive cyber security employing multi-dimensional risk mitigation approaches is key to strong cyber resilience and effective business operations.

WORKING WITH COVID-19

COVID-19 accelerated digitisation and the exposure to cyber risk. In the UK, £34.5 million was reportedly stolen between March 2020 and March 2021 as a result of COVID-19 related fraud[16]. Globally in the Travel & Tourism sector COVID-19 related cybercrime ranged from fraudulent vaccine passports or PCR test results to dishonestly claiming refunds or loyalty points.

> "Ethical and empathy fraud has been more substantial" and working from home "made workers more susceptible to cyber security breaches".
> -Sondra Feinberg at Microsoft

As a result of Covid-19 **Ethical and empathy fraud** may involve threat actors claiming refunds or credit that a travel service did not meet their needs or that they are unable to travel due to COVID-19 reasons when this is untrue.

According to Devon Bryan at Carnival Corporation, "cyber miscreants are opportunistic, and COVID-19 created huge opportunities for them; we saw that in COVID-19 related phishing attacks". Threat actors are agile and will continue to innovate as opportunities to exploit vulnerabilities become available. With pent-up demand for travel and needs to travel for compassionate or business reasons, facilitating travel while protecting public health has been a key priority for the sector. However, changing and inconsistent restrictions create room for attacks. Looking ahead, as travellers continue to be required to disclose large amounts of sensitive identity and health information to facilitate travel, often needing to allow access to an array of smartphone solutions and even download QR codes, these solutions and codes could become compromised and pose a risk for the smartphone and its owner.

> With an almost 74% increase in mobile smartphone users between 2016 and 2017[17] and many organisations adopting a mobile-first approach for marketing and sales, **mobile security** is integral to cyber security. 86% of mobile security experts agree there is moderate to high risk associated with mobile devices and 50% see these risks rising faster than others.[18]

In the case of travel during COVID-19, a Digital Travel Portal[19] for the pre-travel collection and assessment of traveller COVID-19 status information can simplify the process for travellers and governments while collecting and securing personal information and facilitating travel. This, in turn, can help mitigate cyber risks and enhance cyber security for these processes.

At the same time, the move to **remote working**, which has involved the increased use of personal and mobile devices, has increasingly placed responsibility for company cyber security on employees. While in-office organisational cyber ecosystems tend to be secure this security had previously not been extended to employee homes. As noted by Daniel Dobrygowski at the World Economic Forum, "every home office had become a vector for potential cyber attackers". Threat actors who had accessed home or public Wi-Fi networks may have used this as an easier path into organisational systems, requiring organisations take a more holistic approach to cyber security. While organisations cannot ensure the security of home or public Wi-Fi networks, staff training can further protect employees in their use of IoT devices.

Cyber risks resulting from COVID-19 should not be seen as separate to organisational risk, including cyber risks associated with hybrid work models. As a sector that has managed risk across various regions, Travel & Tourism leaders have found ways to secure networks in spite of geographical challenges. Indeed, "strong operating principles should be clear from across the globe" says Michael Jabbara at Visa. As such, these operating principles and security measures can and should be expanded into employee homes. What is more, for cyber resilience, organisations will need to expand threat monitoring to include potential attack entry points through home and public Wi-Fi systems.

MANAGING GLOBAL LEGISLATION

The evolving cyber landscape necessitates specific cyber laws to enhance civil protections. While no legislation for cyber security exists at a global level, laws are enforced at regional and national levels. These tend to fit into three broad areas at present.

While the European Union has taken a regional approach with the General Data Protection Regulation (GDPR)[20] countries including South Africa and Australia have implemented a national approach with the Protection of Personal Information Act (POPIA)[21] and the Privacy Act[22], respe ctively. In the United States, laws exist at both federal and state levels. The depth to which legislation addresses cyber resilience differs by region and even country. In some regions legislation specifically addresses cybersecurity and resilience while in others it is included in other laws. What is more, legislations have, at times, been complemented by certifications, with countries in some cases making the completion a key requirement for organisations with government contracts, such as in the UK. In effect, while some laws and certification criteria may have similarities, there is no global standard. Each country and/or region determines its own legislation and associated consequences for non-compliance.

For a sector that operates across the globe, such as Travel & Tourism, compliance with various cyber laws is a necessity and can become complex in the absence of global legislation. For most organisations, compliance with the most rigorous regulations has been the best approach as it creates an effective baseline. Certifications tend to be determined by need, with the completion of these certifications made a requirement by specific governments or organisations. In most cases, best practices, such as multi-factor authentication and staff training, support compliance with legislation while also forming a crucial part of cyber resilience. These are complemented by "robust software and learning counter-measures", according to Nobuaki Fukumoto at JTB, as they support regulation compliance as well as cyber security and resilience.

According to Kelly White at Mastercard: "There's innovation in regulation." This has been seen in the shifting approaches to cyber security in response to regulations as well as innovative cross-border collaborations such as the Global Cyber Alliance[23]. whose founding organisations include law enforcement. With the support of legislation and compliant organisations, there has been increased transparency around data usage and cyber security, which continues to empower employees and consumers with knowledge on what data is being used and how. This transparency is a key aspect of building trust which can complement long-term resilience.

Despite a fragmented global approach, the sector continues to collaborate across the public and private sectors to share threat information and improve global cyber protections and resilience. As cyber risk constantly evolves and adapts, this collaboration will be key to ensuring the long-term resilience of Travel & Tourism.

These tend to fit into three broad areas at present: privacy, critical infrastructure, and supply chain

Privacy: laws and regulations that seek to govern the fair collection, usage, and disposal of personal data. Travel & Tourism organisations often process large amounts of sensitive data and so need to comply with these.

Critical infrastructure: ensuring that organisations and systems critical to the operation of a state maintain the appropriate level of security (physical and cyber). Aviation, ground, and maritime transportation fall into this category in many jurisdictions.

Supply chain security: ensuring consistency in security and hygiene practices throughout the supply chain. Following some high-profile cyber security issues introduced through the supply chain many global organisations are considering legislation around the supply chain.

GOOD PRACTICES

Cyber security is a key aspect of operational resilience. Effective security measures can help build and strengthen cyber resilience to further ensure an organisation can recover from a cyberattack.

> "Cyber resilience is not about helping our organisation to recover
> from but battle through a cyber-attack".
> -Devon Bryan at Carnival Cruises

As the sector adapts and looks for new opportunities for growth beyond the recovery from COVID-19, much has been learnt about the key role of cyber security in maintaining business continuity. To further enhance cyber resilience, this section outlines the practical application of seven good practices. These have been recommended by industry experts and can be implemented to help prepare for and withstand an attack while laying the foundation to support long-term cyber resilience.

1 **Integrate cyber risk management into organisational risk management**. While risk exists, it can be managed through the assessment, prioritisation, and implementation of effective mitigation measures. Given the significance of digital solutions in business operations, cyber risk should be prioritised and managed along with other business and operational risks. Consider what additional measures are required for OT systems. While cyber risks require the support of experts, they are the responsibility of the business as a whole. Understanding the changing threat landscape to consider possible entry points and new threat tactics and mitigations is important. Risk management processes should be reviewed and updated regularly to ensure the appropriate investments are made. Budget should be allocated according to the risk level and mitigation measures required to ensure maximum protection and limit exposure in the case of a breach. Hire skilled professionals to create and inform cyber risk policies, understand and implement best practices, and manage risk proactively and continuously. Integrating cyber risk in business strategy is a foundational aspect of resilience.

2 **Educate and train all staff**. Training and education are key to onboarding new staff and ensuring the effective use and adoption of new systems and processes. As digital acceleration has continued to propel organisations into increased usage of connected systems to enable business operations, refine customer experiences, and enhance productivity, effective cyber security education and training is paramount. In an increasingly digital world, the usage of digital systems has been largely seamless; appropriate education and training on the risks digital may introduce should be prioritised at the same rate and proportion, if not more so. Not all members of staff will require the same cyber security training as each team or member will have a varying level of risk exposure based on their job function and the data this requires them to access. However, each staff member should be trained in the core principles of cyber security and understand the organisational approach to data protection and cyber security. Training should be comprehensive to ensure staff understand what risks exist and how to mitigate them. It

should be tailored to employees and their risk level to appropriately equip staff members with the tools to mitigate their specific risk. Review and update training regularly to maintain relevance and effectiveness and integrate it in the organisation's broader health and safety protocols. Through training, the number of attacks caused by compromised or careless insiders can be decreased significantly.

3   **Expand risk protections beyond the physical workplace.** Historically, many cyber security controls were designed around the physical office and working environment. As the adoption of cloud and mobile technologies grew this began to change with the need to provide protection anytime, anywhere, and in any place. With the move to remote and hybrid working, this approach should be updated as it assumes risk is only relevant at the physical office. Cyber controls should be applied more broadly. Employees now have access to corporate systems through company-owned and personal devices and from locations within and outside the physical office. Consider how hybrid working models could affect security and heighten vulnerabilities, and, specifically, factors that could compromise cyber security. These include home Wi-Fi security, employee cyber hygiene on their own devices, and accessing systems from public locations. It is important to ensure that the protections against these risks do not rely on connection into the office. This includes ensuring that employees only have access to the data they need to do their job and core systems have strong protections in place. Consider the most probable risks and those with the highest impact. Be proactive in risk management and address potential risks as soon as possible.

4   **Employ a zero-trust approach to cyber security.** The challenges of securing the modern mobile and connected workforce has led to increased focus on zero-trust as a way to manage cyber security and build resilience. This moves away from previous approaches that implied higher levels of trust for connections within the organisation. While the zero-trust principles are not new, they reflect the strong application of core cyber security principles that may have been more loosely applied when controls were not available. Its pillars are the explicit verification of requests to access resources; implementation of the principle of least privilege access to limit users' access rights to what is strictly required to do their jobs; and assumes a breach or compromise so that no system or connection is assumed to be clean. Using the zero-trust approach can help enable more flexibility in access whilst limiting the exposure of core systems. This approach can even be applied to OT and IoT systems where zero-trust controls may need to be applied at the network level through the segmentation of systems and continuous monitoring for vulnerabilities.

5   **Employ ongoing threat assessments,** build relationships with leaders in the field, and use analytics to refine cyber protection measures. Equip cyber experts to find security vulnerabilities by performing threat actions and penetration tests to help the mitigation of risk and build resilience. As much as possible, segment systems to avoid breaches compromising the entire cyber ecosystem and mitigate risks of double extortion. Prioritise mission-critical systems and manage their access and protection accordingly to ensure little to no downtime for essential business operations. Build relationships with experts in the field, from national cyber security centres such to private sector industry leaders, to share intelligence and advice. National cyber security centres such as the Government Communications Headquarters (GCHQ) in the UK, and the National Counterintelligence and Security Centre (NCSC) in the US can act as valuable resources and partners in countering cybercrime.

6   **Be transparent.** While trust in Travel & Tourism is high, and security is assumed and often seamlessly incorporated, cyber security should not be concealed. Effective cyber security measures ensure the protection of personal and payment information, and their presence reinforces this objective and builds trust. Clearly notify employees and customers of implemented security measures and enhancements as they occur and be open about the reasons for data collection, data usage, and the period for which data will be stored. By only using the least amount of required personal data and payment information while offering the highest protections, organisations can foster trust while limiting organisational risk and the risk to the data owners. As appropriate and required, highlight compliance with legislation and standards as well as the implementation of best practices to help educate staff and customers. Where applicable, immediately notify affected parties and regulatory bodies of any breaches and remedies taken to mitigate the impact of the breach. While a breach can cause immense harm, how an organisation effectively resolves it and recovers from it can enhance future resilience.

7   **Implement an organisational standard.** Legislation differs globally and business leaders should determine how their organisations operate and comply with legislation in their regions of operation. For businesses operating in diverse regions, with varying compliance requirements, an organisational standard can foster a standardised approach to cyber security that complies with legislation while enhancing data protection. To determine these standards, consider applicable legislation in the

regions the business operates, and the controls required to comply. This will provide a global list of controls that the organisation should apply. In many cases, compliance with the legislation in one location, such as privacy requirements for example, may enable global compliance. However, the creation and implementation of an organisational standard may require regional modifications to address local cultural contexts or legislation. These modifications should be informed by cyber security, privacy, and legal experts and remain subject to review and revision as necessary. If necessary, modify the standard for the regional context while ensuring those modifications do not contradict the organisational global standard. Communicate the implementation of these standards with employees and customers, and, if required, make the standards available to regulators to demonstrate compliance.
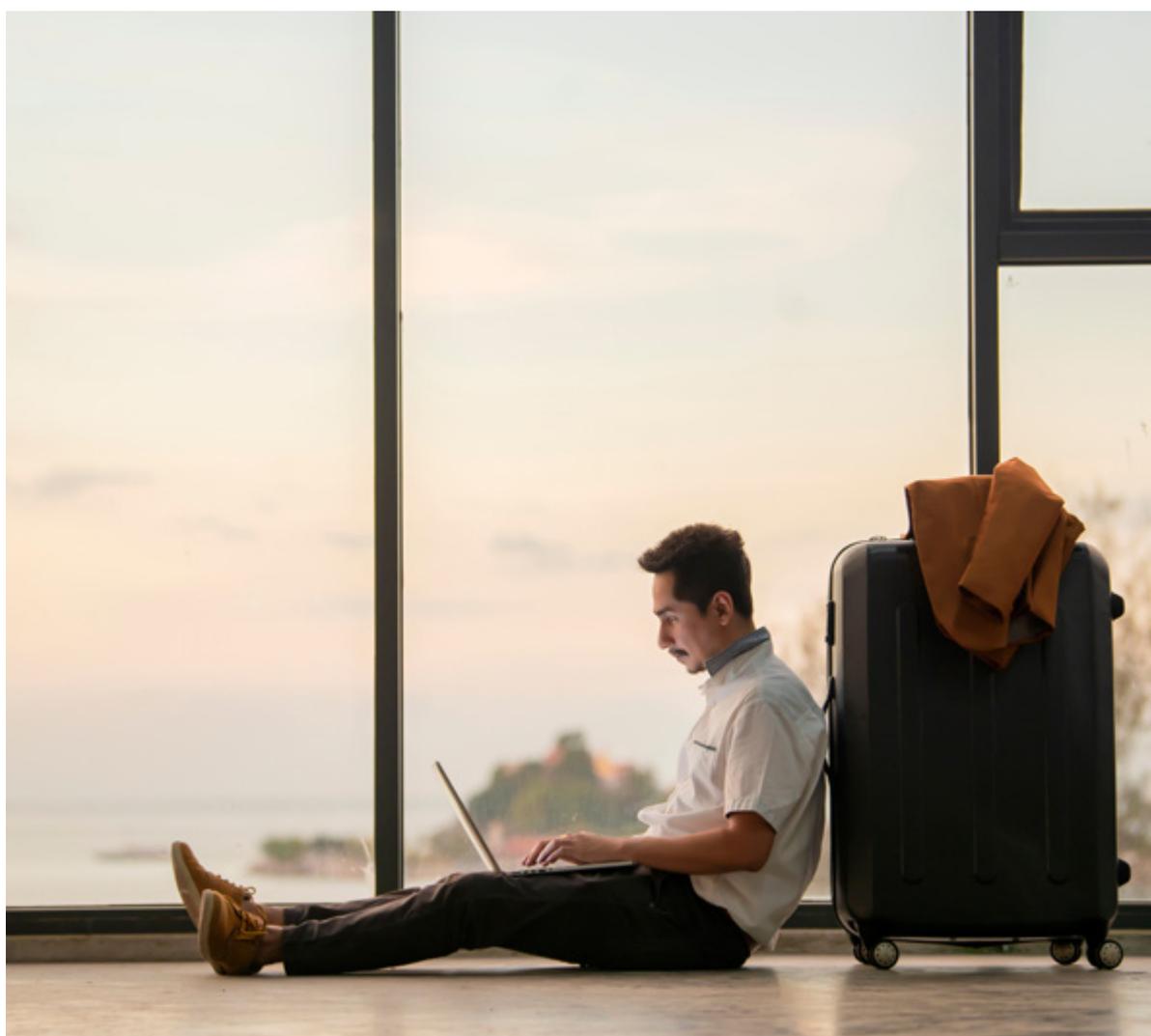
LOOKING AHEAD

The speed at which cyber security threats materialise and evolve coupled with the Travel & Tourism sector's global reach and distributed nature can make cyber resilience a complex challenge. With its access to personal and payment information and the requirement to store and transport this information across digital systems and regions, the sector's risk of cyberattack requires an approach that not only protects against those attacks but prioritises resilience. What is more, the pervasiveness of digital systems to enable a more efficient system for businesses and seamless experiences for travellers has ensured cyber is a significant aspect of most business operations and human life.

However, while this challenge is not insurmountable; it requires collaboration, innovation, and compliance. In past decades, malicious software has been made easily and freely available as has information about how systems can and have been breached. Through communication and knowledge sharing, the number of organisations breached, and the scale of those attacks can be decreased substantially. Effective and regular threat monitoring ensures these risks can be identified, assessed, and effectively managed.

Looking ahead, cyber threats will grow in complexity and range as digitisation continues to enhance business operations. The ability to refine how the Travel & Tourism sector operates will be enhanced by cyber interventions, making effective cyber security protocols and high-level prioritisation vital. Through this prioritisation and the proactive efforts of business leaders and cyber experts, cyber resilience can be enhanced and adapted as the risk landscape evolves. Indeed, some risks are specific to organisations and thus require a specialised approach; the opportunistic nature of threat actors and the high cost of targeted attacks have shown that lessons learnt from other cyberattacks have lessons for other organisations in preparing for and mitigating future risks.

Legislation enhances civil protections and provides a framework for compliance for the private sector. Governments play a key role in determining and enforcing these standards and implementing consequences for non-compliance. Indeed, global legislation differs, with no single global standard, and governments manage legislation within their jurisdictions as appropriate. The private sector is exposed to a range of threats and tactics and is crucial in identifying malicious activities and finding innovative mitigation measures that can be replicated in other organisations and regions. Threats vary and evolve but through the lessons and expertise of other organisations and the implementation of standards and zero-trust approaches, they can be managed and mitigated for the benefit of the sector as a whole. As a result of COVID-19 cyber risks have evolved, and the risk landscape has expanded exponentially providing a larger and more complex risk landscape. The move to hybrid and work-from-home models has further altered the risk landscape and created additional potential entry points for threat actors, requiring a more holistic and proactive approach to security to ensure maximum risk mitigation and minimum impact in the event of an attack.

Cyber resilience is integral to the future of Travel & Tourism as cyber systems continue to facilitate and enhance business operations and customer experiences. While organisations cannot predict all future attacks and the malicious methods through which they may be performed, understanding the nature of cyber risk and threat actors can enhance how business leaders and cyber experts can effectively prioritise cyber security and resilience. For the sector to continue its recovery from COVID-19 and enhance its resilience for the future, it must integrate cyber security and cyber resilience in its recovery efforts. As pivotal as digitisation has been to the sector's growth and ongoing recovery from COVID-19, it will be increasingly foundational to its long-term growth and resilience as the move to digitisation accelerates and expands.

ACKNOWLEDGEMENTS

IMAGES

P1: FLY:D, Unsplash
P2: Luca Bravo, Unsplash
P3: Jacob Lund, Shutterstock
P4: Jezael Melgoza, Unsplash
P6: Dotshock, Unsplash
P8: Jacob Lund, Shutterstock
P11: Joshua Earle, Unsplash
P13: Shine Nuca, Shutterstock
P14: Annie Spratt, Unsplash
P15: Yousef Alfuhigi, Unsplash
P19: FLY:D, Unsplash

SPECIAL THANKS

The authors would like to thank the following people and members, as well as numerous contributors from Microsoft and the World Travel & Tourism Council for their contributions to this report

Julie Shainock
Global Managing Director of Travel & Transport, Microsoft

Shane O'Flaherty
Global Director of Travel & Transport, Microsoft

James McDonald
Director, Safe & Seamless Travel, World Travel & Tourism Council

Alain Simon
Director of Network Services, Amadeus

Greg Sullivan
Chief Information Officer, Carnival Corporation

Devon Bryan
Global Chief Information Security Officer Carnival Corporation

Anudeep Parhar
Chief Information Officer, Entrust

Matthew Vaughn
Director Aviation Cyber Security, International Air Transport Association

Manon Gaudet
Assistant Director Aviation Security and Cyber, International Air Transport Association

Nobuaki Fukumoto
Chief Information Officer, Chief Information Security Officer, JTB

Jack Kumada
Tourism Marketing & Research Executive Director, JTB

Kelly White
Senior Vice President, Chief Executive Officer, RiskRecon – A Mastercard Company

Dan Johnson
Vice President: Digital Identity, Cyber & Intelligence Solutions, Mastercard

Sondra Feinberg
Director of Partners and Alliances at Microsoft Fraud Protection Solutions

Simone Fortin
Global Head of Cyber Security, MSC Cruises

Deneen DeFiore McGarvey
Vice President & Chief Information Security Officer, United Airlines

Michael Lemberger
Senior Vice President – North America Risk Officer, Visa

Michael Jabbara
Vice President, Visa

Daniel Dobrygowski
Head of Governance and Trust, Centre for Cybersecurity, World Economic Forum

---

The World Travel & Tourism Council is the global authority on the economic and social contribution of Travel & Tourism. WTTC promotes sustainable growth for the Travel & Tourism sector, working with governments and international institutions to create jobs, to drive exports and to generate prosperity. Council Members are the Chairs, Presidents and Chief Executives of the world's leading private sector Travel & Tourism businesses.

For further information, please visit:
WTTC.org

Endnotes

1. The Cyber Resilience Centre of the Southeast (2021) The South East tourism industry re-opens but cyber criminals are not taking a break. Available at: https://www.secrc.co.uk/post/5-tips-to-drown-out-cyber-criminals-from-your-business (Accessed: January 2022)

2. Ponemon Institute (2019) 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. Available at: https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf (Accessed: January 2022)

3. Inc. (No date) 60% of Companies Fail in 6 Months Because of This (It's Not What You Think) Available at: https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html (Accessed: January 2022)

4. Accenture (2019) Ninth Annual Cost of Cybercrime Study. Available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (Accessed: January 2022)

5. CyberSmart (2021) Cyber security in hospitality – a growing issue? Available at: https://cybersmart.co.uk/blog/cybersecurity-in-hospitality-a-growing-issue/ (Accessed: January 2022)

6. FCM Travel (No date) Why Cyber Security is the Fastest Growing Source of Travel Risk. Available at:https://www.fcmtravel.com/en-us/resources/insights/why-cyber-security-fastest-growing-source-travel-risk (Accessed: January 2022)

7. IATA (2020) Fraud in the airline industry – why carriers need to think of themselves as crime fighters. Available at: iata_whitepaper_fraud_july2020_digital (Accessed: January 2022)

8. Cabinet Office (No date) The cost of cybercrime. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf (Accessed: January 2022)

9. IBM (2021) How much does a data breach cost? Available at: https://www.ibm.com/security/data-breach (Accessed: January 2022)

10. Security Today (2020) The IoT Rundown For 2020: Stats, Risk and Solutions. Available at: https://security-today.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2 (Accessed: January 2022)

11. CyberCrime Magazine (2020) Cyber Crime to Cost the World $10.1 Trillion Annually by 2025. Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Accessed: January 2022)

12. WEF (2022) Global Cyber Security Outlook 2022. Available at: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (Accessed: January 2022)

13. IBM (2021) X-Force Threat Intelligence Index. Available at: https://www.ibm.com/downloads/cas/M1X-3B7QG (Accessed: January 2022)

14. Tessian (2022) Must-Know Phishing Statistics: Updated 2022. Available at: https://www.tessian.com/blog/phishing-statistics-2020/ (Accessed: January 2022)

15. FCM (2019) Wi-Fi is a business traveller's best friend – or is it? Available at: https://www.fcmtravel.com/en-au/travel-news/wifi-business-travellers-best-friend (Accessed: January 2022)

16. BBC News (2021) Covid fraud: £34.5m stolen in pandemic frauds. Available at: https://www.bbc.co.uk/news/technology-56499886 (Accessed: January 2022)

17. WTTC (2021) Digital Solutions for Reviving International Travel. Available at: https://research.wttc.org/digital-solutions-for-reviving-international-travel (Accessed: January 2022)

18. GDPR (No date) What is GDPR, the EU's new data protection law? Available at: https://gdpr.eu/what-is-gdpr/ (Accessed: January 2022)

19. https://www.gov.za/documents/protection-personal-information-act (Accessed: January 2022)

20. Australian Government (2022) Privacy. Available at:https://www.ag.gov.au/rights-and-protections/privacy#:~:text=The%20Privacy%20Act%201988%20(Privacy,and%20in%20the%20private%20sector. (Accessed: January 2022)

21. Global Cyber Alliance (No date) Available at: https://www.globalcyberalliance.org/ (Accessed: January 2022)

22. Oberlo (2021) 10 Mobile Usage Statistics. Available at: https://www.oberlo.co.uk/blog/mobile-usage-statistics (Accessed: January 2022)

23. Verizon (2021) 2021 Data Breach Investigations Report. Available at: 2021 Data Breach Investigations Report | Verizon (Accessed: January 2022)