White Paper

HardenStance

Cyber Security After the Pandemic

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

CYBER THREAT ALLIANCE JUNIPER NETWORKS NETSCOUT paloalto NETWORKS

April 2021

Executive Summary

- Core principles of enterprise cyber security best practise had to be temporarily overlooked in the stampede to remote working and cloud service adoption that followed the COVID-19 lockdowns of March and April 2020.
- Fixing those mistakes to get cyber security posture back to pre-pandemic levels has been preoccupying security teams. But as the peak of the crisis passes, there's an opportunity to exploit the impact of the pandemic to improve cyber security posture.
- The pandemic's legacy for cyber security should be a secure innovation culture; convergence of network and security at the edge; better segmentation of network domains at home; and concerted action against ransomware.

An Impact across Many Cyber Security Disciplines

The cyber security industry has faced two major sets of challenges over the last twelve months. The attacks and exploits affecting Solar Winds, Accellion, Microsoft and their customers have focused attention on supply chain risk, but the impact of the coronavirus pandemic has been felt more broadly across cyber security domains and disciplines.

Maintaining business continuity was critically dependent on undertaking this urgent logistical and operational upheaval quickly and with minimal disruption.

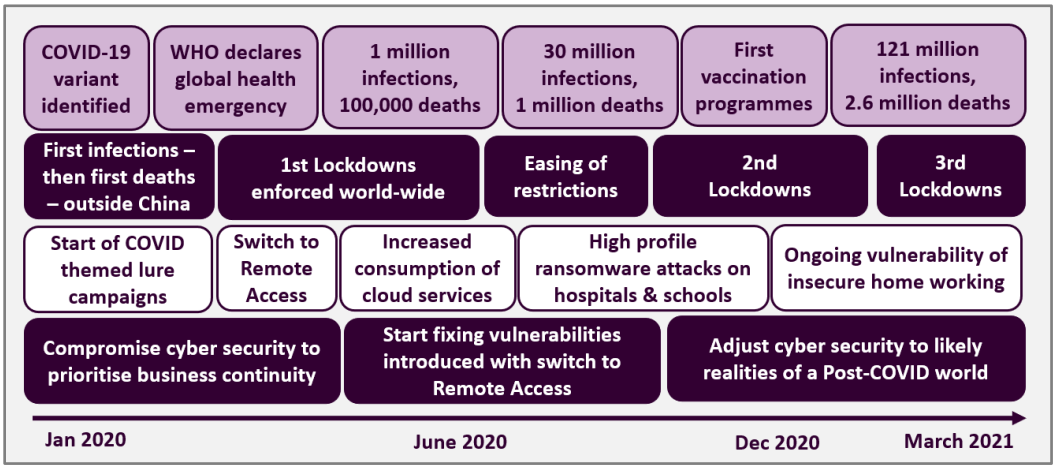
This White Paper reflects on the impact of the pandemic. One year on from those first major national lockdowns or 'stay-at-home' orders of March 2020, it reviews the ways in which organizations adjusted their IT architecture and working practices to the circumstances of the pandemic - and how their cyber security posture changed with it. With some countries finally daring to hope that the peak of the crisis - measured in COVID-related death rates – may have passed, this paper also points to what the lasting effects of the pandemic on cyber security best practise are going to be.

The National Lockdowns of March-April 2020

It's worth recalling the intense pressures that the first national lockdowns brought to bear on the IT sector. In some sectors of industry and for some job roles, IT professionals that were supporting maybe 10% or 20% of their organization's employees working remotely some or all of the time had to rapidly flip that ratio on its head so that most or nearly all employees could work from home all of the time during lockdown.

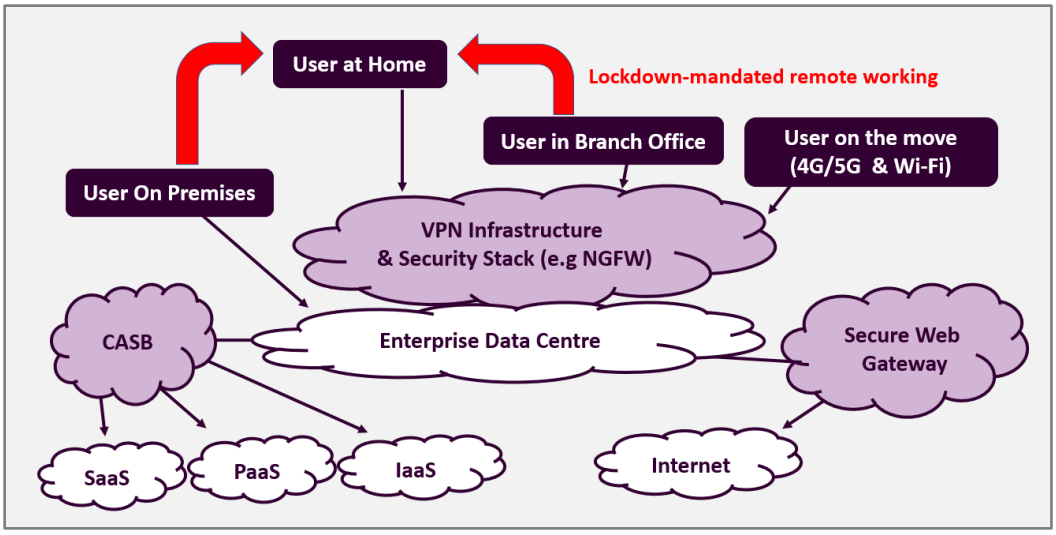
It's hard to overstate what a big ask this was for those enterprise IT teams that had planned for something like a pandemic – let alone for those that hadn't. This switch to remote working had to be undertaken in days – in some cases literally overnight. Maintaining business continuity – the number one priority – was critically dependent on undertaking this urgent operational upheaval quickly and with minimal disruption.

Figure 1: Pandemic Milestones & Resulting Cyber Security Challenges



Source: HardenStance

Figure 2: Lockdowns Drove a Rapid Change to Remote Working



Source: HardenStance

Investment in Remote Access Infrastructure

In the case of most large organizations, the wholesale change that IT and network teams had to introduce to their architecture and service models was driven by a lot of investment in two primary components - Remote Access infrastructure as well as cloud and cloud-delivered services.

The despatching of entire development teams to work from home meant that a lot of mature cloud migration plans had to be abandoned in favour of a 'lift and shift' approach.

They invested heavily in their Remote Desktop Access (RDA) servers, Virtual Private Network (VPN) concentrators and Remote Access routers. This was needed to support a two, four, six, eight or ten-fold surge in remote sessions hitting the data centre. With intensive adoption of video apps like Skype and Zoom by so many newly set-up homeworkers, enterprise WAN and LAN capacity had to be upgraded as well. Invariably this also triggered the need to change other aspects of IT and network infrastructure such as routing and DNS resolution paths.

Accelerated Adoption of SaaS and Cloud Services

The second big change that had to happen, out of necessity, was an acceleration in the adoption of Software as a Service (SaaS) and cloud services. The shift to Remote Access drove a huge upward spike in enterprise consumption of SaaS applications. This was seen in the case of well-established business apps like O365, Salesforce, Workday and Concur but it was most noticeable in the case of on-line collaboration tools like Slack, Microsoft Teams and Zoom. Driven by consumer as well as enterprise spending, Zoom's revenues for the quarter ending 31 January 2021 were $882.5 million, up from $188.3 million for the equivalent quarter in the previous year.

The despatching of entire development teams to work from home (along with almost everyone else) meant that a lot of mature cloud migration plans comprising detailed design, develop, test, deploy and review phases planned to stretch out over months or years had to be abandoned. Many IT teams saw little choice but to change tack completely and downgrade to a much more basic 'lift and shift' approach. Dropping largely unmodified legacy apps into the cloud according to an Infrastructure as a Service (IAAS) model meant foregoing many of the benefits of being in the cloud – but it did at least have the advantage that it could be done in days or weeks.

Vulnerabilities & Attack Vectors of the Pandemic

The changes introduced with the first lockdowns necessarily required risk to be taken with cyber security. There isn't enough reliable data to quantify this effect accurately – in part because so many flaws and violations are not measured (or even known about). But that doesn't mean we can't be confident that on the whole, enterprise security posture was knowingly relaxed in the early stages of the pandemic.

Any change in business processes inevitably introduces some cyber security risk. Far-reaching change that is introduced rapidly, and under intense pressure, is almost guaranteed to introduce quite a bit more than that. Faced with lockdown, most organizations judged – probably correctly in most cases – that leaving large numbers of employees unable to access business data and applications for days or weeks posed a bigger threat to the business than temporarily relaxing security policies and allowing the threat surface of their organizations to expand. Decisions were often expressly supported with the stated intent that exposures would be fixed retrospectively, once the immediate threat to business continuity posed by lockdown had passed.

This section describes the increased cyber security risk that many organizations found themselves vulnerable to arising from the effects of the pandemic. It also describes the ways in which threat actors adjusted their Tactics, Techniques and Procedures (TTPs) to exploit these new gaps in security.

Staff were permitted to connect their own personal devices to the corporate network, leaving the business exposed to whatever endpoint security was (or wasn't) running on them.

Tooling Up the Workforce from Their Living Rooms

Most organizations were not ready for most or all of their staff to be despatched to their homes. Keeping their people operational meant relaxing all manner of important aspects of cyber security hygiene, rules and policies, including the following:

- Staff without employer-supplied PCs were permitted to connect their own personal devices to the enterprise network, leaving the business exposed to whatever endpoint security software and patching schedule was (or wasn't) running on them.
- Employer-supplied computers were exposed to risk from new home workers using them for personal use, like clicking on a phishing link within their personal email.
- Irrespective of the device being used, all employees were accessing the enterprise network remotely, leaving the business at the mercy of whatever security was (or wasn't) supported by the Wi-Fi network in the home or coffee shop.
- Key security policies like only allowing company-approved USB devices to be connected to computers or even blocking USB ports altogether had to be relaxed – for example, where employees needed to print from their home printer.
- The home router, complete with whatever security features it did or didn't have, became the new enterprise edge or security perimeter. Remote Access and cloud has been eroding the perimeter for years but the pandemic finally killed it off. More accurately, IoT 'things' connected to the home router – a connected doorbell or washing machine – became the new enterprise perimeter by virtue of these devices sharing the home router with computers used for work.
- As they always have, most VPNs tended to grant open, indefinite, binary, permissions to access whole suites of corporate applications or data assets, with no contextual verification checks or other security updates.

Employee Susceptibility to Stress - and Complacency

There would have been risk attached to loosening security controls in this way for the minority of staff that worked remotely before the pandemic struck. These individuals tended to be more senior and comparatively knowledgeable about the risk to their employer associated with them working remotely.

But these additional risks had to be taken with a much larger influx of staff. These tended to be both more junior and less familiar with enterprise security risk. They were also asked to adapt to Remote Access norms in unprecedented times when they themselves were vulnerable to high stress.

Human vulnerabilities amongst the huge new influx of remote workers added to cyber security risk in the following ways:

- People adapting to using a new communications tool like Zoom don't necessarily think to use adequate authentication to protect their employer against eavesdropping or disruptive 'Zoom-bombing'.
- People don't necessarily think to prevent their children or partners from using employer-supplied or employer-authorized personal devices, with the attendant risk of them viewing sensitive data or the device becoming infected.
- For some employees, circumstances at home makes remote working very stressful. These individuals tend to be a lot more susceptible to both benign errors and malicious insider threat behaviours. At the same time, the comfort of their own home and the absence of office peer-pressure can also cause happy and fulfilled employees to relax their cyber security disciplines.

Stressed home workers tend to be a lot more susceptible to both benign errors and malicious insider threat behaviours.

Reduced Visibility and New Working Norms for SOC Teams

Last but not least, the work of a Security Operations Centre (SOC) itself underwent substantial disruption arising from lockdowns – in terms of what the SOC was seeing as well as how analysts were able to going about responding to it.

It was common for SOCs to lose some amount of visibility into their organization's traffic arising from the shift to remote working. Efforts needed to be made to capture logs from personal devices connecting to the enterprise network, albeit within constraints determined by employee rights to privacy. Also, logs and telemetry generated by SaaS applications look very distinctive from a SOC perspective. Adapting to that is challenging when businesses start using SaaS applications for the very first time. It's also challenging when the SOC is accustomed to SaaS applications accounting for a given share of the application traffic mix, only for that share to suddenly spike upwards.

SOC Analysts Have Had to Work from Home too.

More than that, the SOC team has faced further challenges by virtue of SOC analysts themselves being despatched to work remotely. Substantial adjustments have been required arising from analysts no longer being able to use the big screens of the SOC environment; restrictions on the use of high-end servers for correlation work in some cases; not to mention having to forego the inter-personal, on-site, teamwork that characterises the exhaustive investigation and resolution of some SOC alerts. Some analysts, some entire teams, have found this adjustment easier than others.

Threat Actors Adjusted to New Opportunities

Inevitably, threat actors have adjusted their sights to exploit the new vulnerabilities. What follows here is a summary of some of the adjustments threat actors have made to the pandemic into which cyber security defenders and users have some visibility.

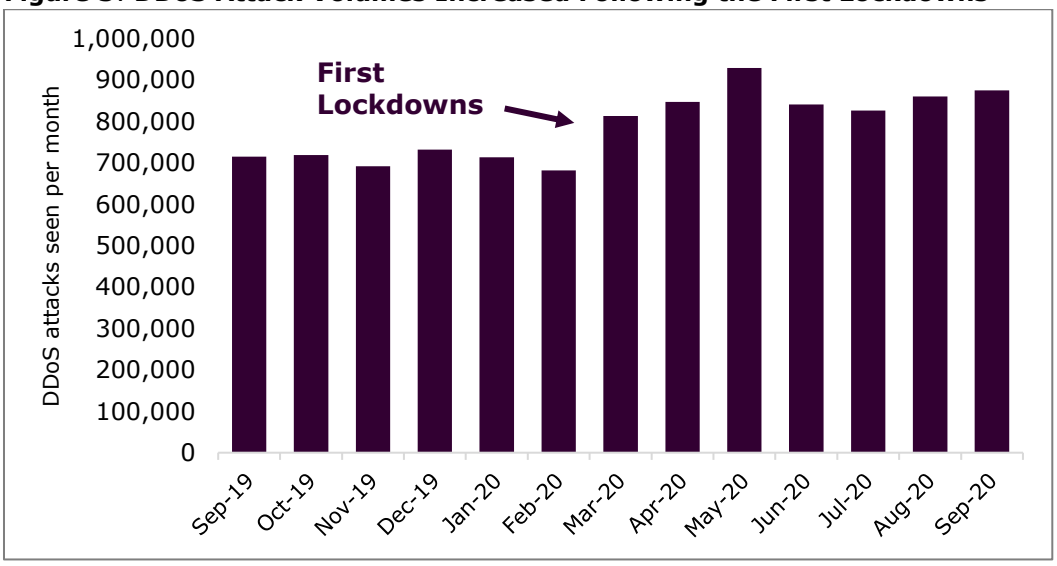
- **A shift in lure attacks to COVID-19 themes**. Among the most common have been email, SMS and other messaging-borne lures whose themes have evolved with different phases of the pandemic. Initially these exploited shortages of Protective Personal Equipment (PPE). This evolved to fraudulent contact tracing messages or notifications of government fines for breaching lockdown rules. More recently the emphasis has shifted to lures promising access to vaccines. This can be expected to evolve further with new phases, such as availability of 'vaccine passports.'
- **DDoS attacks that exploit Remote Access Overhauls**. As shown in **Figure 3,** data from leading DDoS protection providers points clearly to an overall spike in the volume of DDoS attacks immediately following the first lockdowns. It also points to adjustments in the TTPs of DDoS threat actors.

  One example is an uptick in the targeting of on-premises VPN concentrators because the shift to remote working has meant that an attack can disrupt an entire organization whereas before it might only have disrupted 10-20% of the workforce. Another is a spike in the abuse of RDP for brute force RDP attacks as well as for User Datagram Protocol (UDP) reflection and amplification attacks. A third example, beginning in August last year, is one cyber crime group's combining of attacks on VPN concentrators with a specific extortion demand in bitcoins. Several vendors report a substantial rise in secondary and tertiary extortion after initial infection.

Ransomware attacks have posed a heightened risk to children and to human life throughout the pandemic.

- **A Ransomware Surge, Heightening Risk to Children and Human Life.** As shown on the next page, ransomware attacks have posed a heightened risk to children and to human life throughout the pandemic. A marked rise has been observed in threat groups exfiltrating files with a view to leaking them in an effort to incentivize victims to pay. Earlier this year, the leader of the REvil threat group boasted in the media of hacking into providers of ransomware insurance in order to target their clients. This raises the spectre that buying ransomware insurance can

Figure 3: **DDoS Attack Volumes Increased Following the First Lockdowns**



Source: NETSCOUT SYSTEMS, INC.

potentially make businesses more rather than less vulnerable to ransomware now. According to Palo Alto Networks threat research group, Unit 42, the average ransom paid has increased by 171% - from $115,123 in 2019 to $312,493 in 2020.

- **Use of Stolen PII to Steal Coronavirus Relief Payments**. In an August 2020 report, the U.S. Department of Labour's Office of Inspector General (OIG) estimated that at least $26 billion could be lost to American taxpayers due to cyber criminals claiming coronavirus relief payments with stolen identities.

Aggressive Targeting of the Healthcare and Education Sectors

Data released by different security vendors all point to a large increase in ransomware attacks over the last year. And attackers have used the disruption of the pandemic to specifically target the healthcare and education industries a lot more aggressively. Calculating that the pressure of trying to save lives under intense stress would increase their willingness to pay, some ransomware gangs have been targeting the healthcare sector on an unprecedented scale.

Attackers have also tested the assumption that schools and universities will be more willing to pay up to get all their data back when everyone's learning remotely than they would when everyone's on campus. And why would an anti-socially inclined student be content with a pre-pandemic prank of merely disrupting school with a DDoS attack on its website or internal systems when instead a pandemic-era DDoS attack on Remote Access infrastructure can take down lessons between every single teacher and every single student in the whole school?

A Marked Spike in Ransomware Attacks on Hospitals and Clinics

Following a number of ransomware attacks, the FBI and other federal agencies warned on October 28th last year of "an imminent cybercrime threat to U.S. hospitals and healthcare providers". One attack that preceded that announcement was a September 23rd Ryuk ransomware attack on Universal Health Services (UHS), a Fortune 500 company, serving around 3.5 million patients a year through 400 healthcare facilities in the U.S. and the UK. Among other U.S. facilities hit by ransomware during the pandemic have been Sky Lakes Medica Centre, Klamath Falls, Oregon and Canton- Potsdam, Massena and Gouverneur hospitals in New York. Hospitals in Brno in the Czech Republic and Saraburi Hospital, Thailand, were also hit, as was the World Health Organization (WHO) itself. Targeting healthcare facilities posed a risk to human life before the pandemic (which is why, historically, most ransomware gangs steered clear of them). The risk is substantially increased during a pandemic so there can be little doubt that the ethical boundaries have been redrawn by some ransomware gangs.

Old and New Types of Cyber Attack on the Education Sector

All remote and on-site classes in Buffalo Public Schools in Buffalo New York were cancelled on March 15th and 16th due to a ransomware attack on March 12th. Ransomware has also featured prominently among attacks that have disrupted Huntsville City School, Alabama; Baltimore County Public Schools; Clark County School District, Las Vegas, Nevada; and Athens Independent School District, Athens, Texas. On September 3rd last year, police arrested a 16 year old at South Miami Senior High School. He admitted to using DDoS attacks to render the Miami Dade school district's remote learning platform almost unusable. As recently as March 16, 2021, the FBI formally advised schools in 12 U.S. states, as well as in the UK, of a heightened risk to educational establishments from ransomware.

Enterprise Security in the 'Post-COVID World'

As set out in this paper, most organizations went from IT services architecture and security posture 'Model A' in February 2020 centred on the enterprise premises to 'Model B' by the end of March or April centred on the home. At least two factors have rendered both a return to 'Model A' and a long-term commitment to 'Model B' highly inadvisable. Many countries were subjected to second lockdowns at the end of last year. Recently, some countries have even entered their third. The extreme weighting of both models renders both of them not fit for purpose as organizations emerge from the pandemic.

Ever since April 2020 a critical question has therefore been what should a new target 'Model C' look like for a 'post-COVID' world? The signs are that many positive first-time experiences of home working seem to have triggered a decisive shift in favour of more remote working. This is reflected in the attitudes of U.S. business executives from a January 2021 PWC survey shown in **Figure 4**. It's hard to predict exactly what new patterns of remote working will look like. In technologically advanced markets, it could go to 30-40% of employees working mainly from home, or even higher. What does seem pretty clear is that it won't revert back to pre-pandemic levels – or anything like it.

Ransomware attacks have posed a heightened risk to children and to human life throughout the pandemic.

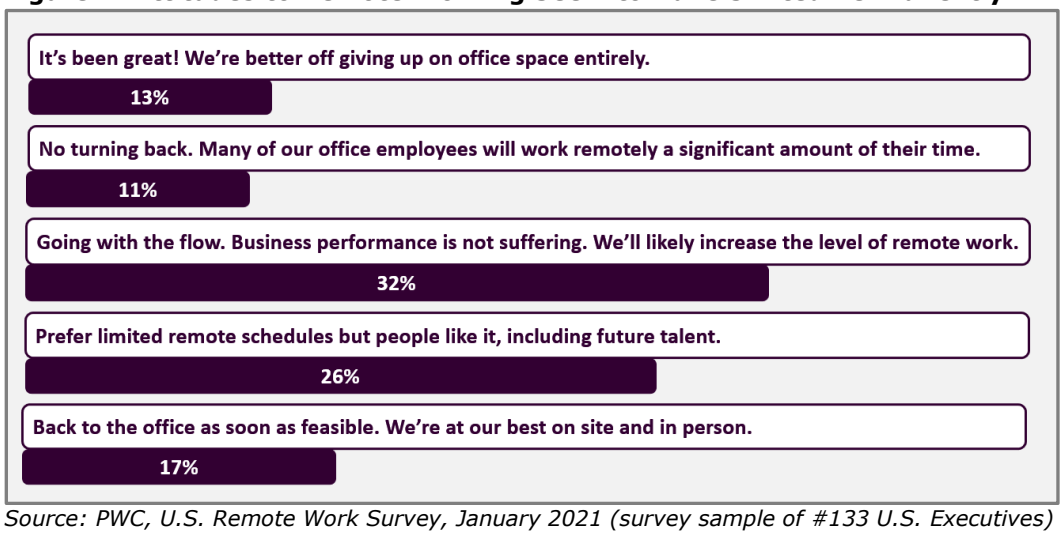
Short-Term Fixes and Longer Term Strategies

Some organizations began planning and even executing on this almost as soon as their Remote Access transformations were complete last April. Others have started turning to it more recently or are waiting for the crisis to pass before defining new goals and next steps. There are two aspects of adjusting cyber security to the post-COVID world. The first consists of plugging the holes in the model that emerged after the first lockdowns. That involves going back and fixing routine technology hygiene like implementing cloud security controls in development environments; ensuring exposed VPN concentrators aren't easy to identify by attackers doing reconnaissance; and upgrading to a dedicated DDoS protection capability rather than relying on necessary but insufficient DDoS protection features embedded in a Next Generation Firewall (NGFW).

The second aspect of the adjustment consists of developing a longer term strategy. Some foundational principles should guide enterprise security thinking here:

- It's not possible to know exactly what the post-pandemic business world will look like, except that the current crisis will pass and the impacts will play out over years.
- Waiting for perfect clarity to emerge from the prevailing fog of uncertainty carries too much risk. Absolute clarity very rarely presents itself – and even if it does, waiting for it risks leaving current shortcomings in place for far too long.

Figure 4: Attitudes to Remote Working Seem to Have Shifted Permanently



Source: PWC, U.S. Remote Work Survey, January 2021 (survey sample of #133 U.S. Executives)

- A start can be made just by defining the target architecture and operating model and the core principles needed to achieve it. It's not realistic to expect to nail down every detail of every means to every end before taking a first step.

Four Recommendations Arising from the Pandemic

HardenStance believes organizations should adjust to the permanent changes to cyber security brought about by the pandemic by adopting four specific recommendations. They may be new or new-ish in some respects. But for the most part, they should be familiar. These recommendations are singled out and elaborated on here because they have become even more relevant now than they were - and because the risk of disregarding them has gone up as a direct result of how the pandemic has changed how business is done. The recommendations are itemized below, then discussed in turn:

1 Build a Business Culture around Secure, High Velocity, Innovation.

2 Design for Converging Network and Security at the New Edge.

3 Segment Business, Private and Government Domains Better.

4 Support Concerted Action Against Ransomware.

Those that didn't see enough value in cyber attack planning and response rehearsals before March 2020 should be a lot more persuaded by now.

1. Build a Business Culture around Secure, High Velocity, Innovation

A lot of building blocks determine exactly how security and business continuity does – or doesn't – permeate an organization's work culture. The legacy of the pandemic points to the need for change across a number of them.

- **'Wargaming'**: Before the pandemic, organizations will have either invested a lot, a bit, or not at all in business continuity planning, cyber attack response plans, and other types of 'war-gaming'. There can't be much doubt which type of company has fared best during the pandemic, in terms of both the speed of their immediate response to lockdowns and the probability of mistakes being made (known as well as unknown). As General Eisenhower put it, "the plan is nothing; planning is everything." The pandemic brought home to most organizations what a crisis looks like up close and personal - as well as what's required of a rapid response under intense pressure. Those that didn't see enough value in cyber attack planning and response rehearsals before March 2020 should be a lot more persuaded by now.
- **Employee Training**: The principle that all employees are an organization's "first line of cyber security defence" and that "cyber security is a team sport" also predates the pandemic by a couple of decades. Again, though, the scale of the long-term shift to remote working makes employees that don't practise good security hygiene in their homes a significantly greater risk than before the pandemic when they were office-based.

  Experience during the last year has showed that there's no one size fits all here. It may be appropriate to lure some employees in some roles in some industries into clicking on a mock phishing link to test their security awareness. Luring other types of employee into clicking on a link for a fictional company bonus payment at a time of high stress can easily trigger humiliation and alienation rather than positive engagement. Organizations should also be willing to invest in more engaging formats including gamification of training programs.
- **Exemplary Leadership**: What's sometimes missed with employee training is the importance of leaders living and breathing the values of cyber security hygiene – and being seen to live and breathe those values every day. The stakes are simply higher now. Those leaders that were excused for not doing enough to motivate themselves and their teams on this should not be excused now.

- **Recruitment Diversity**: Increased levels of remote working also represent an opportunity for businesses to look beyond the most popular locations for recruiting cyber security talent. That can deliver greater diversity within the security team - potentially at lower cost too.
- **The role of the CISO**: The role of the Chief Information Security Officer (CISO) started out as a highly technical, somewhat reactive role, focused on identifying technology vulnerabilities and implementing technology rules to mitigate them. For some years it has been on a path of evolving to a more strategic business level role of understanding, evaluating, communicating and managing cyber risk to management and the board, such that in some organizations the CISO's role is on a par with the Chief Information Officer's (CIO's) now. Consistent with that the role has tended to become more proactive and more tightly coupled with Business Continuity Planning (BCP) as well as day to day operations. By bringing pre-existing dependencies between cyber security and IT, network, business strategy and BCP functions into such sharp relief over the last year, a legacy of the pandemic is that it is likely to accelerate this evolution in the way the CISO's role is defined.

The CISO's role could become merged along with CIO, BCP and other roles into a unified role of Digital Process Officer.

  Broadly speaking, this is likely to take one of two different forms. One may be nothing more than an acceleration in the rate at which the CISO's role is elevated in importance. Alternatively the role could become merged along with CIO, BCP and other roles into a unified role of Digital Process Officer or Cloud Technology Officer. The potential advantage of this approach is that it allows accountability for multiple key processes to revenue within the business to be converged under one role and one department rather than being fragmented across different roles.
- **Threat Intelligence Sharing**: One other aspect of cyber security working practises that should be informed by learnings from the pandemic is the value of threat intelligence sharing. Given that hospitals in Europe, the U.S. and Asia were all struck by a ransomware gang believed to be operating out of Europe, some key sectors of industry should be asking whether – and if so how – they can improve cyber threat intelligence sharing within their specific industry across international boundaries.

2. Design for Converging Network and Security at the New Edge

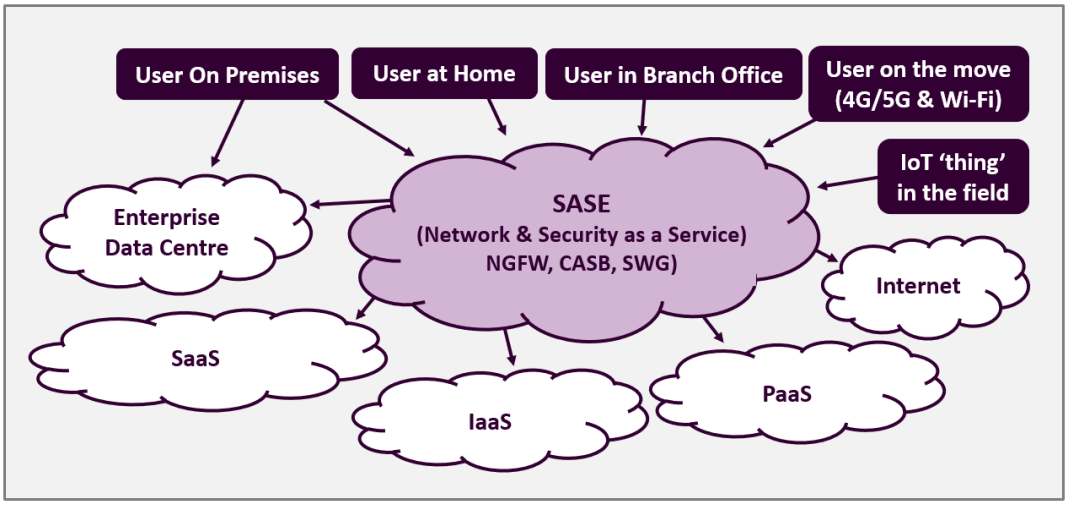
The steady flight of employees, data and apps away from the enterprise premises to remote locations and the cloud drove recognition of the shortcomings of centralized VPN architectures years before the pandemic.

VPNs fall short in terms of network cost, flexibility and scalability – why backhaul traffic to the data centre if it's destined for the cloud? VPNs fall short in terms of security too. They encrypt traffic between endpoint and data centre but most allow a user to access whole suites of business applications and data via a one-time authentication. They're typically not subject to any granular monitoring or reauthentication and vulnerable to hijacking by threat actors.

Going back a few years, organizations began complementing or substituting their VPN investments with SD-WAN. Leveraging MPLS, 4G, 5G and public internet services, SD-WAN on its own can certainly relieve the network access shortcomings of VPNs but it doesn't address the security flaws. Hence the two years leading up to the pandemic saw a concerted move by vendors to integrate security controls into SD-WAN portfolios. They also saw the emergence of the Secure Access Services Edge (SASE) solution category.

As shown in **Figure 5** on the next page, SASE converges network and network security into a unified cloud service that delivers connectivity with application-aware routing and security to any enterprise branch, employee's home or employee mobile device. Rather than being automatically backhauled to a VPN concentrator, the traffic is routed with relevant security by the SASE platform directly to wherever it is that the relevant applications are hosted.

Figure 5: The Pandemic Has Enhanced the Business Case for SASE



Source: HardenStance

From a security perspective, SASE solutions comprise core functionality like NGFW, Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) as a baseline, along with other capabilities. Over time, Zero Trust Network Access (ZTNA) should become a critical component of SASE. Once a user is connected to those applications they are authorized to access, ongoing context-based validation and security monitoring can be applied on a per-user and per-application basis, albeit this needs to be as non-intrusive as possible.

The characteristics of SASE make it ideally suited to serve as the target architecture for the post-pandemic 'Model C' .

The big challenge with Zero Trust is that while it's a compelling-sounding principle, most businesses need a very much better understanding of what's required within their own environment – basic building blocks like well managed active software directories and appropriate data classifications, for example.

The characteristics of SASE make it ideally suited to serve as the target architecture for converging network and security at the edge according to the post pandemic 'Model C', identified earlier. SASE had strong momentum in terms of mindshare leading up to the pandemic and is emerging from it even stronger. But fulfilling all of its promise will be the work of several years.

3. Segment Business, Private & Government Domains Better

This paper has shown how the pandemic has accelerated the convergence of personal and employer applications and data on the same home network and on the same devices. As has been alluded to, a number of different steps and approaches can be taken to segment the two domains, but security teams typically find themselves having to adopt approaches that are heavily customised.

The coming months are therefore likely to see the emergence of more integrated, 'out of the box' approaches to addressing segmentation of home networks. Approaches centred on configuring the home router have to contend with consumer privacy laws. Application-centric approaches like SASE should evolve to support tighter integration with endpoint security.

There's potentially a third key actor in the mix here as well. Whether it be in relation to so-called 'Track & Trace' applications or 'Vaccine Passports', governments may emerge from the pandemic with more by way of legitimate rights to deliver and monitor applications on citizens' personal devices on either a voluntary or even a compulsory basis. Accelerated investment in vendor roadmaps to meet the segmentation and micro-segmentation requirements of all legitimate stakeholders in the data and applications that run on personal devices will be another legacy of the pandemic.

4. Support Concerted Action Against Ransomware

This paper has shown how cyber criminals have targeted – and continue to target – hospitals during the pandemic when the risk to human life arising from disruption is so much greater than normal. As mentioned, there are signs that this is viewed, including by many governments, as having "crossed a line".

There is an opportunity for businesses to seize on this momentum and work with security vendors, industry associations, business organizations and government to take more effective action against ransomware gangs. One example is the new Ransomware Task Force that was set up in December 2020. It compromises nineteen security vendors and cyber security industry associations.

There are several policy directions this can go in, some of which may be less problematic now than they were twelve months ago. One example is the idea of extending Know Your Customer (KYC) transparency rules in financial transactions to the cryptocurrency domain that ransomware gangs depend on for untraceable payments. While legitimate privacy-related objections are still an important consideration, the new landscape looks more promising for advocates of this type of measure now.

Somewhat perversely, a decisive shift in the way ransomware attacks are addressed across government and industry has potential to be a positive outcome of the pandemic from a cyber security perspective. But businesses do need to be proactive and lend their support to make that happen. ■

About the Sponsors

The sponsors of this White Paper are Cyber Threat Alliance, NetScout Systems Inc, Juniper Networks and Palo Alto Networks.

About Cyber Threat Alliance

The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. We take a three-pronged approach to this mission:

1. Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.

2. Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3. Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow on a global basis, enriching both the quantity and quality of the information that is being shared amongst its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operational collaboration to enable a more secure future for all. For more information about the Cyber Threat Alliance, please visit www.cyberthreatalliance.org

About NETSCOUT SYSTEMS, INC.

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius™ service assurance solutions provide real-time, contextual analysis of service,

network, and application performance. Arbor Smart DDoS Protection by NETSCOUT products help protect against attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets.

To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions powered by service intelligence can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

About Juniper Networks

Juniper Networks challenges the inherent complexity that comes with networking and security in the multicloud era. We do this with products, solutions and services that transform the way people connect, work and live. We simplify the process of transitioning to a secure and automated multicloud environment to enable secure, AI-driven networks that connect the world. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on Twitter, Linked In and Facebook.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. www.paloaltonetworks.com

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, The GSM Association and ETSI. HardenStance is also a recognized Cyber Threat Alliance 'Champion'. To learn more visit www.hardenstance.com