The human variable: Designing a security strategy for a future in flux

Received (in revised form): 18th May, 2021

Gary Sorrentino
Global Deputy CIO, Zoom Video Communications, USA

Gary Sorrentino currently serves as global deputy CIO for Zoom Video Communications. A former managing director for J. P. Morgan Asset & Wealth Management, Gary was the global head of client cyber awareness and education. For over 12 years, Gary was the chief technology officer for J. P. Morgan AWM's global technology infrastructure initiatives, where he managed its data privacy programme and was responsible for infrastructure, application and end user technology production support. In 2014, he assumed a new role as the lead for its cyber security efforts and developed a company-wide 'protect the client' cyber programme designed to raise cyber security awareness among employees and clients. With almost 40 years' experience in information technology, Gary has served in various other IT leadership positions in firms across the financial services industry. Prior to joining J. P. Morgan in 2005, Gary was head of global infrastructure and head of technology efficiencies at Citi Private Bank, where he was responsible for global infrastructure support and strategic technology initiatives. Other roles he has held include global technology CFO at Credit Suisse and North America IT controller at UBS.

E-mail: gary.sorrentino@zoom.us

Abstract The hybrid workforce is no longer a concept, it is a reality. But as employees embrace new working environments and flow in and out of the office, this hybrid approach poses a unique challenge for security leaders. This paper explores how organisations will need to create a security strategy rooted in the variability of the hybrid workforce — one that meets employees where they are and helps them learn the role they play in securing this new model. This strategy is rooted in three key principles: adopt a zero-trust approach, personalise data protection and bolster hands-on, robust training. Readers can expect to learn what it really takes to put this approach into practice — and what threats and roadblocks they should anticipate along the way.

KEYWORDS: hybrid workforce, security strategy, zero-trust approach, data protection, security training

INTRODUCTION

The COVID-19 pandemic shattered everything we knew about the modern-day office. Companies did not have a business continuity plan that took into account conditions where knowledge workers and clients were forced to work remotely, concurrently, and for an extended amount of time. When we sent employees home, our entire IT strategy and support model had to pivot practically overnight. We were not checking what workers took when they left, or what equipment they already had in their homes. We focused on finding quick solutions to secure the at-home office, ensuring employees could still collaborate while keeping crucial information secure. But a remote, distributed workforce has led to its fair share of headaches for IT; since the start of COVID-19, there has been a 35 per cent increase in IT incident tickets per day, according to HappySignals.[1] While IT has had to move swiftly to operationalise a remote workforce and keep employees productive and secure, it is going to have to revolutionise operations to prepare for the emerging hybrid workforce.

The pandemic spawned a more geographically diverse workforce. People were no longer concerned about being close to the office; they moved out of certain regions, applied and accepted jobs out of state, resulting in the emergence of the work-from-anywhere model. Now, as we approach the next phase of this experience, we are starting to realise remote work will no longer be exclusive to the pandemic, but it will rather be the norm. According to Smartway2,[2] 92 per cent of employees want flexibility around where they work, with 40 per cent wanting to work mostly from home with occasional office time. Employees want to decide when they work, how they work and where they work. With employees' appetite for flexibility, leaders everywhere are examining what it means to establish a successful and secure hybrid workforce.

In fact, we are all discovering the emerging hybrid workforce at a different rate — some countries, states and industries sooner than others. Many companies have tried to return to the office with limited success. In some countries, there is no date when it will happen, only when it is deemed safe for some people to go in. Even then, it could depend on job function, personal preference, family matters, geographic location, safety best practices and company policy. Some jobs, functions and tactics are better carried out virtually than in-person, and vice versa. The office will represent something new entirely, as employees can now do the same work at home that they used to do in the office.

With the hybrid workforce, there will be three types of workers IT teams have to factor for: some who go to work every day, some who are remote and some that are a mix of both — probably the most complex group. With the latter group, work is also going to be from anywhere, meaning airports, outposts, hotels, etc. Exposure points will become exponential, and IT will have to prepare for a diverse set of environments to secure and control. This begs the question: how do you successfully manage the fluidity of workers, with information travelling in and out of offices, airports, hubs, coffee shops and libraries at different rates?

Rather than build separate security policies for those at home and those at work, we need to embrace a strategy that addresses all three groups. This strategy needs to be agile in the way we track data, monitor activity and identify any irregularities. We need to know who is working where, when they are working, how they are working and what they are working on.

Organisations will need to create a security strategy rooted in the variability of the hybrid workforce — one that meets employees where they are and helps them learn the role they play in securing this new model, while still keeping them productive and effective. Leaders must make infrastructure and processes flexible, adaptable, and tailored to the human variable.

IT leaders can start by laying a foundation rooted in three key principles:

- Adopt a zero-trust approach;
- Personalise data protection;
- Bolster hands-on, robust training.

Let us dive into what that means.

ESTABLISH ZERO-TRUST AS A STANDARD

Today's users face more complex threats than ever before. Threat actors have become creative and have taken advantage of the pandemic — who has not received a fake COVID-19 testing e-mail, a text that your package has been delayed or a phone call for contact tracing? These days, phishing attacks are more personalised, malware has become stealthier and ransomware continues to surge. In fact, according to the IBM 2021 X-Force

Threat Intelligence Index,[3] ransomware was the top threat type, comprising 23 per cent of attacks. Sodinokibi (REvil) ransomware alone reaped a conservative profit estimate of US$123m.

As both the threat landscape and workforce evolve, so must IT policy. Pre-pandemic times still saw enterprises deploying perimeter security, where the focus was on setting up techniques at the perimeter of a network to secure data and resources. This approach relies on systems such as firewalls and browser isolation systems, and focuses on threat recognition, surveillance detection and pattern analysis. But this castle-and-moat approach was rendered useless in the face of COVID-19 and will be ineffective with the hybrid workforce. As employees roam in and out of the office, travel around the world and take their devices with them, IT has to deploy a zero-trust model. We are no longer just protecting a business's four walls — it is every four walls for every employee wherever they go.

A zero-trust model is the only sustainable route for the hybrid workforce. It is a micro-segmentation approach, tracking users, their locations and other data to determine whether to trust a user, machine or application that is requesting access to certain data. Zero-trust draws on technologies such as multi-factor authentication, identity and access management (IAM), encryption, scoring and file system permissions and additional factors. Some of these techniques may feel expected to employees, while others may require an explanation as to why they are important and necessary. To enable easy adoption of a zero-trust approach, explain the situational relevance in layman's terms to show employees the power and potential consequences of their own action — for example, we require single sign-on because your password is still your dog's name, or simply changing a number in your password will not be enough. From there, you can put the policy into practice.

Additionally, we should be training users to operate as minimalists — they should always try to accomplish a task with the least amount of access to assets possible. Do you really need to print that document at home? Do you have to make that confidential phone call from a coffee shop? Make users become self-aware about their own security, inspire them to become the chief information security officer (CISO) of their own life.

As bring your own device (BYOD) becomes the norm, IT teams must strategically leverage these personal devices to enforce a zero-trust policy via multi-factor authentication and relevant policies. Constant authentication and validation feed into existing user habits, with people already persistently checking their phones. By making multi-factor a prerequisite for any user-related business functionality, you underpin security beneath everything that user does, no matter where they are working from or what they are working on.

IT should also encourage employees to stay vigilant of any suspicious activity to their mobile devices and routinely check which devices are registered under multi-factor authentication, ensuring they recognise all the devices registered under their account. In today's sophisticated threat landscape, cybercriminals may find ways to register a phone number or another device to an account, potentially surpassing corporate multi-factor authentication as a result. While this does not uncut the necessity of multi-factor authentication, it does mean the zero-trust approach needs to seep into this aspect as well. By routinely vetting registered devices and being aware of changes to your mobile device, end user security can be on par with some of the most advanced attacks out there.

PERSONALISE DATA PROTECTION

Data protection and privacy are fundamental to every organisation, regardless of where and how employees access information. While data security has always been more focused on big breaches, IT now needs to focus on contextual endpoint security to be able to scale data protection to meet the needs of an everywhere workforce. Establish defined principles and outcomes for how data is handled per type of environment — any type of environment you think an employee may work from. For instance, data handling is different when employees are in a controlled office scenario or home versus a coffee shop.

Beyond that, IT teams need to deploy programmes that will secure every device in every instance, such as a mobile device management (MDM) strategy. A comprehensive MDM programme establishes a foundation for a future in flux. Work with a trusted vendor to deploy on-device applications and configurations, corporate policies and certificates and backend infrastructure to simplify device management and create visibility into endpoint security. IT teams must, however, balance the use of MDM protection with employees' personal device use.

With MDM managing and securing employees' mobile devices — laptops, smartphones and tablets — regardless of the mobile service provider or operating system in use, it offers personalisation without sacrificing comprehensive protection. Employees get to work on the device of their choice and the applications they are familiar with, while IT gets to have a holistic view of every endpoint.

Since employees' devices will live on both corporate and personal networks, IT teams need to also remember that protection for both network types is a necessity for data security.

When it comes to personal networks, IT should educate employees on how to secure their home networks and encourage them to follow simple best practices, such as changing default passwords and keeping firmware up to date. IT must also ensure a virtual private network (VPN) option is a standard for all employees, but especially for those who jump back and forth between the office and home and are constantly on the go.

To protect in-office employees, IT teams should deploy agile networking solutions that offer real-time monitoring, anomaly detection, micro-segmentation and quarantined networking. The use of unregistered devices should not be permitted on corporate networks.

Monitoring and detection should be supported by a security operations centre (SOC) designed for this new workforce as well. While many turned to a virtual SOC in the COVID-19 era, IT teams of larger organisations with flexible budgets should consider embracing a new type of SOC that empowers them to scale as the workforce does. A hybrid SOC combines in-house operations with virtual, outsourced operations, with some members of the IT organisation handling key focus areas while others provide a certain breed of additional support. A hybrid SOC can aid with out-of-office, 24/7 and global coverage, as well as enable in-house IT to focus on more strategic tasks while the outsourced members handle issue remediation.

CREATE TAILORED, EXAMPLE-BASED TRAINING

Human nature is the weakest link in any security strategy; the IBM 2021 X-Force Threat Intelligence Index[4] reports 95 per cent of cyber security breaches are due to human error. That is why training, testing and security awareness are and will continue to be paramount.

Training and continuous learning help employees understand the role end users play in the overall security posture of an organisation. This creates a sense of responsibility and accountability, showing that company viability is contingent on proper security etiquette and adherence to policies and procedures. Training and awareness also create a culture of security, where all parties feel invested and responsible in the overall protection of an organisation, even if they are disconnected from a physical location.

Basic training can no longer be the only option for combatting today's advanced threats — it needs to be immensely improved. Enhanced security training has to be table stakes for all companies going forward.

Not only do employees need continuous learning on threat detection and data protection best practices, but also training on any technology that enters a business's infrastructure. We need to ensure that any technology we bring in is a user-friendly platform that has adequate controls that make sense to the people who administer and use the technology every day. Implementation should be paired with dedicated tutorials and hands-on training sessions on the software.

While users need to be trained on controls, they need to also understand any changes and threats that may affect the technology they use every day. Whether it is a bug in a new OS or an advanced malware strain, employees need continuous education on what to look out for and what proactive measures they can take to prevent issues.

Hands-on learning will also be fundamental to securing the hybrid workforce. IT needs to build scenarios tailored to the variability of a distributed workforce: build out lessons that speak to the threat of information flowing in and out of the office, to the dangers of working from public areas, to the kinds of attacks that target at-home workers, and more.

Training should be example-based, real-life and unpredictable scenarios, so the lessons feel applicable to users' lives. Create a memorable experience versus a quarterly task that employees feel obligated to participate in.

These scenarios should cover the following:

- *Shoulder surfing*: One of the most relevant threats to the hybrid workforce is shoulder surfing. With employees constantly on the move and working from unique locations, it is more likely that outsiders will be able to peer over their shoulder to see the confidential information on their screen. Say an employee is working in a coffee shop on a laptop, or on their phone on a plane, and the person sitting behind them or next to them has full visual access to confidential information on their screen. When they go for a refill or go to the bathroom, do they lock the screen? Probably not. Has the shoulder surfer seen their password by now anyway? Probably.

  That criminal could grab the device, access the unlocked screen or type in the now-known password, and head to the user's e-mail, which is likely not password protected. The criminal can easily search for key elements such as the word 'bank' and forward those financial e-mails to a burner e-mail account. What is more, if the shoulder surfing incident does occur on a plane, the hacker could forward the info to someone on the ground who can hack into the account while the user is still in the air, since they do not have any service to receive the fraud alerts.

  Hybrid workers need shoulder surfing training to remind them to always be aware of their surroundings, lock their screen, use a screen blocker and make sure no one can see their passwords when they input them;
- *Business e-mail compromise*: A business e-mail compromise is a type of fraudulent attack in which criminals manage to either break into an e-mail account or mimic an e-mail account and successfully pretend to be a certain user. This could be as simple as swapping or misspelling one letter in an e-mail account. As a convincing and common attack, business e-mail compromise is the reason behind most wire frauds. With workers busy and on the go, they need to be reminded to always remain sceptical when someone e-mails them asking for confidential information,

money or access to important business documentation;
- *Elicitation*: In elicitation attacks, criminals will often mimic banks and call a user to tell them that an unusual activity has taken place on their account, such as a charge to their account for two first-class tickets to Dubai. By presenting a problem and offering help, criminals often entice the user to provide more information about their account in order to resolve the perceived problem at hand. It is important people know that any in-bound communications from something like a bank should be met with scrutiny and always confirmed by looking up the actual customer service information;
- *Brute-force password attacks*: Passwords are hard to remember and keep track of. Plus, password managers can feel intimidating to those who do not understand how exactly they work. This often causes users to create bad habits.

  If users have to change a password every 90 days, they simply tweak one of the numbers or a special character, or just reuse a password from an existing account. With so many passwords living on the dark web, however, all a cybercriminal has to do is use the root of a password to conduct a brute-force attack. The attacker simply checks all possible variations of passwords until the correct one is found. Users need to remember password hygiene is not a nice-to-have, it is an essential part of securing a business.

These scenarios have all happened and will continue to affect employees. It is vital your workforce is aware of these situations before they have to learn the lesson first-hand. Coach them into remaining vigilant and suspicious of anything usual.

The text from your significant other for the streaming service platform may not have come from them, so just pick up the phone and call them to make sure. The e-mail from your lawyer to change the wire transfer account for your new mortgage should have been a phone call, so do not respond over e-mail and rather give their office a ring. That external phone call from an unknown source asking for information about employees from your company should never be responded to, period. Criminals tap into humankind's need for convenience and our eagerness to have something done. Tailored security training reminds us all to slow down, vet any unusual requests and double-check every action we take.

CREATING A CULTURE OF SECURITY

The human variable of the hybrid workforce can either be the biggest threat or biggest competitive advantage to your organisation. Success in today's complex landscape will be determined by how you pivot your strategy around that variable. Security leaders can fear the unpredictable nature of the hybrid workforce or harness the power of human potential to instil security into the fabric of their organisation. Humans often do what is convenient or engaging; security can be both.

While the hybrid workforce means more endpoints and more environments, it also means more opportunities for leaders to instil security as a foundational piece in a company's culture. Security needs to be a prerequisite of a company's culture: tied to employee growth and measurement, threaded into existing company events and supported by the aforementioned foundational principles.

Multi-factor authentication naturally feeds into our relationship with our phones. MDM is a simple yet agnostic application that lives in the background of employees' devices, and scenario-based training and awareness makes the threat feel close to home. These simple principles give employees the flexibility they crave while allowing companies to have the security they need.

With the right mix of process and technology supporting your workforce, hybrid is no longer a novel concept, but rather a sustainable, secure reality.

References

1. HappySignals (2021), 'What Makes Enterprise IT end-users happy?', available at https://www.happysignals.com/happiness-score (accessed 14th June, 2021).
2. Smartway 2 (October 2020), 'Returning to Work Survey', available at https://smartway2.com/download-covid19-survey-report/ (accessed 14th June, 2021).
3. IBM (2021), 'IBM X-Force Threat Intelligence Index', available at https://www.ibm.com/security/data-breach/threat-intelligence (accessed 14th June, 2021).
4. *Ibid*., ref. 3.