TREND MICRO | research

FUTURE/TENSE

TREND MICRO
SECURITY PREDICTIONS
FOR 2023

INSIDE THIS/ REPORT

04 Ransomware

06 Cloud Technology

08 Enterprise Perimeter

10 Social Engineering

12 Blockchain

14 Vulnerabilities

16 Industrial Regulations

18 Cybersecurity Platforms

20 Looking Ahead to 2023

2023 will be remembered as the year when battle lines were drawn, then redrawn, along a threat landscape stuck in a state of in-between: No longer are enterprises scrambling to find their footing amid the disruption caused by Covid-19, but for all this talk of the "new normal,"[1] the world has yet to arrive on the other side of the pandemic. The resulting mass-transition of company assets to digital environments has led to increasingly complicated and layered digital environments that will provide the ideal playground for adversaries looking to prey on any lack of visibility.

As enterprises expand their business — and with it, their attack surface — it's imperative that they don't lose sight of the human element on both sides of a cyberattack: Many workforces have now adjusted to hybrid work setups, but blurring the lines between on-site and at-home work will require security teams to do away with conventional point solution-based strategies if they are to stay on top of any potential entry points for opportunistic attackers. It will be important for the C-suite to maintain a big-picture view of their digital infrastructure with a more holistic approach to security, but emerging threats in 2023 will be ones that resonate with a variety of stakeholders that include security teams, legislators, and end consumers. Companies — or at least, their financial officers — will find themselves caught in the push-and-pull of governments calling for more regulations in data security,[2] and a global economy on the cusp of a recession[3] that is sure to make funding threat prevention and response a challenge.

The coming year will also be a time when enterprises and end-users will step back and reevaluate that which not too long ago seemed like they would become transformative innovations: By 2023, the shine will have worn off the metaverse and non-fungible tokens (NFTs), but the blockchain that powers them will be a safe haven for attackers who want to operate without scrutiny. Public trust in open-source software remains up in the air, as we predict more attackers rushing to cash in on the spate of open-source flaws that are bound to surface, leaving developers in the lurch. Similarly, vulnerabilities that rocked the cybersecurity industry, like Log4Shell, may be in the recent past, but still cast a long shadow over lawmakers and businesses worrying about future open-source woes.[4]

Malicious actors will weather this period of uncertainty by hunkering down and striking at old, but reliable, pain points instead of taking big risks that promise bigger payouts. They will revisit the outdated protocols and devices that enterprises should have rightly seen as dead weight long ago and treat them as fresh attack vectors. Businesses should also be on the lookout for familiar threats in new trappings, as attackers fall back on tried-and-true tactics. The rising complexity of social engineering scams, with their proven track record of exploiting people — the weakest link in any security chain — will continue into 2023, as fraudsters incorporate novel technologies like deepfakes in their schemes to stack the odds in their favor. Likewise, expect more threat actors to adapt old-school techniques into "living off the cloud" attacks[5] that will enable them to commandeer legitimate tools and services as part of their kill chains.

Other cybercriminals will be spending 2023 continuously fine-tuning their methods in a more professional operation. Better-armed security teams and legislators clamping down on crime will finally push beleaguered ransomware actors into regrouping and refining their playbooks — we may even come to see some reinventing themselves entirely into data extortion groups instead.

Their adversaries may be content to wait out 2023 until the next wave of seismic changes, but enterprises can regard the incoming year as an opportunity to lay the groundwork for forward-looking countermeasures that can reduce the blast radius of cyberattacks. Our report provides security insights from our threat experts, with the aim of helping decision-makers make informed decisions and develop a strategic security response that can protect organizations across multiple fronts.

Shapeshifting ransomware business models will become a bigger avenue for data theft and blackmail

The ransomware arena is set to undergo major upheavals in 2023, with malicious actors seemingly beset on all sides: International law enforcement has been cracking down on ransomware activity with the promise of cybercrime-related sanctions, as was the case for Evil Corp[6] and Lazarus.[7] Incidents like the takedown of REvil[8] and the Conti leaks[9] also showed the world that even top ransomware-as-a-service (RaaS) providers are not immune to compromise themselves. On top of these decisive blows to their notoriety, we foresee that the double extortion tactics that were widely adopted among ransomware circles will no longer be the devastating one-two punch they once were, as defenders will continue to build a resilience to ransomware attacks.

These factors will necessitate wholesale changes among ransomware actors, who will have to weigh the benefits between staying the path and pivoting to a new business model. To futureproof their operations, they will seek out new avenues that will allow them to still put their skill sets to use. More mature ransomware gangs — which likely have entire hacking teams at their disposal and for whom data encryption is but one step in their attacks — will be compelled to innovate in the face of these changing times: we predict that some will do away with encryption altogether and focus instead on data monetization, looting infected systems for valuable information like credit card details to sell it off themselves.

Others will pursue a different route and reinvent themselves into purely extortion groups, a strategic move that will allow them to repurpose their attacks and maintain the same kill chain but forgo the ransomware payload. It won't be a total about-face for groups to dedicate themselves fully to this business model, as evidenced by the likes of Conti that already have their own data extortion arms.[10] While it's a deviation from the ransomware playbook, extorting their victims directly will still bag criminals a tidy profit without drawing unwanted attention from the media and law enforcement.

Another way ransomware actors may adapt is by turning their attention to the cloud. With more companies migrating their assets and critical data to the cloud, and Gartner projecting that worldwide spending on public cloud services will reach up to US$592 billion in the coming year,[11] the criminal element will have little recourse but to follow cloud adopters if ransomware operations are to stay relevant and profitable. Cloud environments have typically been spared from such attacks owing to the significant differences between cloud and on-premises IT infrastructures, as ransomware variants were conventionally built to attack the latter.[12] However, this also makes the cloud a rich hunting ground for malicious actors who know that there have yet to be any battle-tested ways to respond to ransomware attacks, especially ones aimed at cloud resources containing persistent data like object storage, block storage, and databases.[13] Cybercriminal groups, like Alert and Monster,[14] that have begun to adopt cross-platform malware frameworks to net victims among both users of Windows and Linux operating systems may already be a precursor to the development of these cloud-aware ransomware variants.

Another way ransomware actors may adapt is by turning their attention to the cloud. With more companies migrating their assets and critical data to the cloud, the criminal element will have little recourse but to follow cloud adopters if ransomware operations are to stay relevant and profitable.

Course-correcting ransomware groups won't be limited to these options; eventually, they will become progressively adept at making business decisions and develop more targeted attacks. These versatile attacks will be built to deploy ransomware if the victim prioritizes uptime, a data extortion payload if brand reputation is the victim's first concern, or provide a clean exit strategy if the cybercriminals decide mid-way that the unwanted attention isn't worth the payoff.

Inconsistent application of cloud technology will hurt enterprises as adoption of new tools increases

Enterprises adopted cloud technology quickly within the past three years, migrating assets and operations to facilitate work-from-home solutions as well as contactless technology. The biggest challenges for businesses, particularly established companies used to more traditional tools, were the speed of migration, adoption of newly created cloud technology, and the integration of these changes into the hybrid work environment. This momentum is only set to continue in 2023; in fact, Forrester projects cloud adoption to continue at an unprecedented pace in the financial and regulated sectors.[15] In light of these changes, the main security issues that businesses should be concerned with arise from the inconsistency of implementation and misconfiguration of cloud technology.

With contributions from

VicOne

We expect that security issues will occur as a result of inconsistent application since many chief information security officers (CISO) are not yet familiar with the new technologies or do not have the bandwidth to oversee all cloud vendors. For example, in terms of data backup: there may be a "restore" option on cloud vendor A and a "restore" solution on cloud vendor B, but both these options could look very different. Are both tested? And is the staff capable of executing both restore processes in parallel? These are the situations that will cause problems for enterprises in the coming year. Asset attributes might also be different from vendor to vendor, and that can cause a lot of issues in a mixed environment.

We also anticipate misconfigurations from the user side, mistakes that inadvertently give attackers an avenue into enterprise systems. Enterprise cloud environments involve multiple vendors with different policies, assets, interconnected services, and resources. Fully understanding and setting up such an environment is difficult in the best of times. And in this climate of fast-paced adoption of new technologies, it is an even more daunting scenario. Misconfigurations are the most significant risks to cloud environments. As we reported last year, 65% to 70% of all security challenges from the cloud stem from misconfigurations.[16]

There may also be some security issues stemming from the developers' side as well. Cloud developers are becoming increasingly agile and may put security on the backburner as they progress with their development. We also anticipate that attackers will take advantage of application and service vulnerabilities for external and internal services, since enterprises may not be on top of patching vulnerabilities in a timely manner.

We will also see attackers taking an old technique called "living off the land" (using the victim's own resources against them) and adopting it for the cloud.[17] In "living off the cloud," an attacker would already have access to a victim's system and can use the legitimate tools covertly for malicious activities. For example, they could direct a victim's backup solutions to download private information into the hacker's own storage destination. This also means hackers will not have to build their own tools or software. Hackers will use this method to remain undetected in a victims' system and make the most of this access.

One new attack surface worth watching out for is cloud application programming interface (APIs) on connected cars. Most new car models have built-in embedded-SIMs (eSIMs) that are used to transmit telematics data, communicate with back-end cloud servers, and create Wi-Fi hotspots, among other functions. Cloud-based back-end server applications include smart apps that can remotely start, stop, unlock a car, and apps for monitoring road conditions. The cloud API is the central character of the whole network architecture. Modern cloud APIs are already highly integrated with the car itself, and we anticipate that attackers will take advantage of the security gaps present in these APIs, particularly since these cars are high-value targets. The Tesla API is a good example of this — access control totally depends on an access token: Once an attacker gets the token, the car is basically theirs. In early 2022, a teen hacker gained control of more than 25 Tesla cars remotely in an experiment, exposing the importance of API tokens to vehicle security.[18]

Asset attributes might also be different from vendor to vendor, and that can cause a lot of issues in a mixed environment.

Cars have become powerful and complicated computer systems and should be secured with the same care as enterprise systems. Connected car applications are new and still being developed, but their capabilities against cybersecurity threats are unclear. Connected cars will also be a system of systems, with multiple vendors providing multiple pieces. Security will be hard to guarantee for each of these vendors.

The enterprise perimeter will expand into the home as users become more comfortable in a hybrid work environment

While hybrid work arrangements were not unheard-of prior to the Covid-19 pandemic, gone are the days when a company's security posture was limited to on-premises networks, with more organizations embracing flexible work models that will be the norm by 2024.[19] A Cisco study shows that these have contributed to employee happiness and productivity, although only 28% of respondents felt that their company was well-prepared for hybrid working.[20]

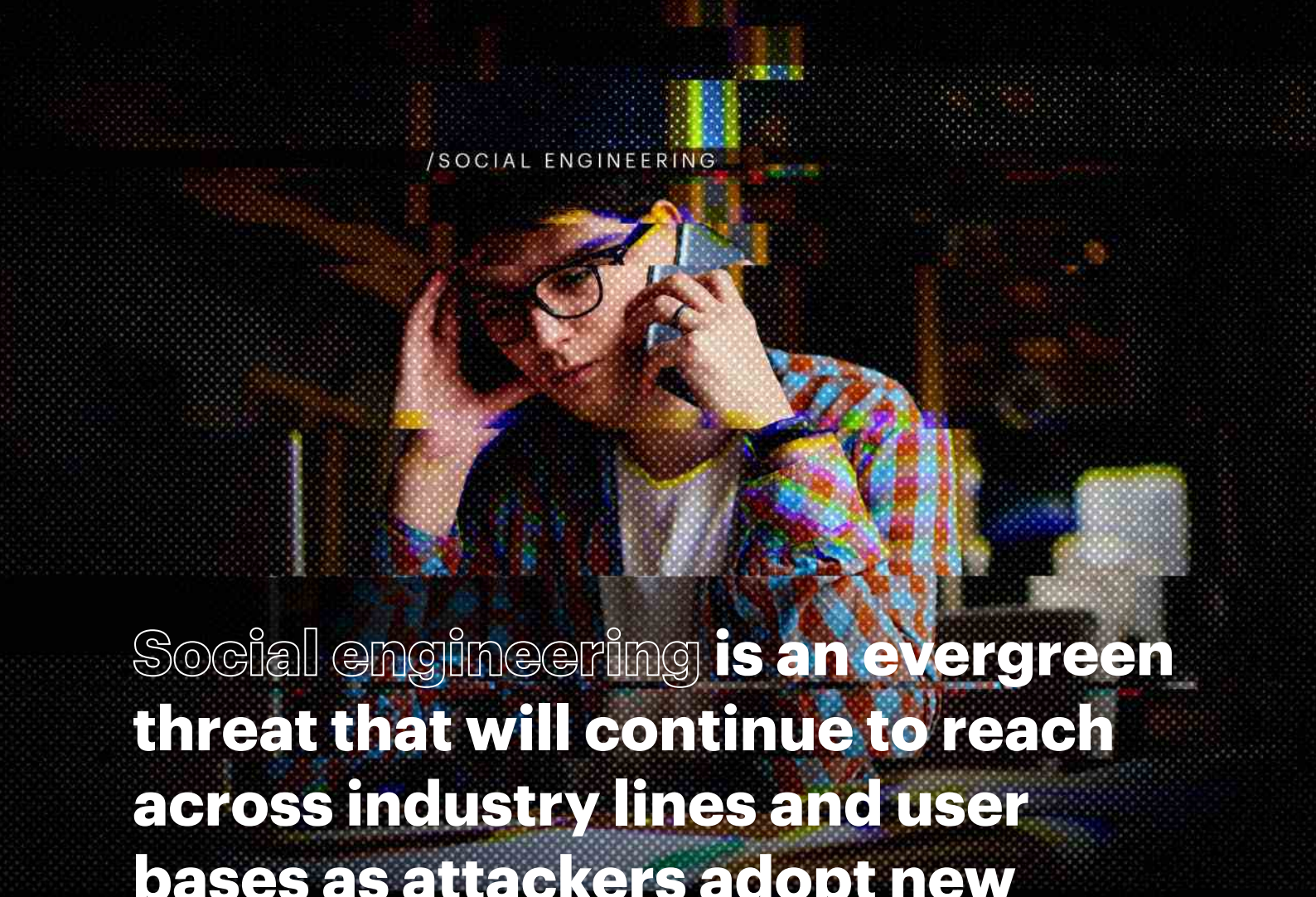
But security gaps are bound to arise from a remote workforce whose devices are constantly moving back and forth between corporate networks and their own home networks.[21] Defenders have limited visibility over the latter, which employees may even share with members of their households — some of whom may also be working for another company. For all its benefits, hybrid work can also run up costly slip-ups: According to a joint study between IBM and the Ponemon Institute, data breaches can cost US$5.54 million on average for companies with at least 81% remote workers, as opposed to approximately US$3.15 million among companies where only half of employees work from home.[22]

Attacks against VPNs soared by nearly 2,000% early into 2021,[23] at a time when lockdowns were in full effect and the world was still struggling to adjust to the changes brought about by remote work. In the year ahead, we expect imaginative cybercriminals to take full advantage of hybrid work setups that are on course to becoming the status quo with a surge of attacks involving network-based worms, or target at-home connections linked to virtual private networks (VPNs) as a means of lateral movement. Doing so will enable them to not only compromise one corporate network but also target other networks down the line to which other household members' devices are connected. For some, old habits die hard, and despite the fact that the Common Vulnerabilities and Exposures (CVE) database lists almost 500 known VPN-related vulnerabilities, a 2022 study conducted by Zscaler and Cybersecurity Insiders suggests that many enterprises continue to rely on VPNs.[24]

Even with mitigation tactics like multi-factor authentication (MFA) that reinforce the barriers keeping attackers at bay, the enterprise perimeter has grown too broad to safely make room for the cloud elements, bring-your-own device (BYOD) policies, and the numerous as-a-service applications that are now common to many businesses undergoing digital transformations.[25] In simpler times, the castle-and-moat security mindset may have sufficed for enterprises, but that may soon change as we expect to see an uptick in the adoption of zero trust models in 2023.

Moving forward, enterprises can accommodate the needs of both their in-office and at-home employees with a zero trust approach. Having a zero trust environment in place where the identity of all devices, users, and apps are assumed to be vulnerable and must be explicitly verified — and even then, are only granted least-privilege access — cuts down the likelihood of bad actors establishing a foothold into a network.[26] Additionally, practicing zero trust network access (ZTNA) gives enterprises an alternative to VPNs that fits in as part of their broader zero trust strategy: Unlike VPNs that provide highway access to the entire network, ZTNA allows authorized users a secure connection to a specific application or service only, preventing threat actors from moving freely across a network.[27]

Various frameworks already exist to serve as a roadmap for different kinds of organizations looking to integrate zero trust into their operations: Forrester's zero trust edge (ZTE) model, for one, outlines how zero trust principles can be applied to cloud security and network services,[28] whereas the National Institute of Standards and Technology's (NIST) zero trust architecture (ZTA) uses zero trust to guide the design of enterprise and industrial systems.[29] Increasingly distributed companies that are on a path to the cloud will also benefit from Gartner's Secure Access Service Edge (SASE), a network architecture model that builds on zero trust principles and consolidates the core functionalities of security and networking technologies including ZTNA, secure web gateway (SWG), and cloud access security brokers (CASB).[30] Because SASE can also be deployed in a single software stack, enterprises will be able to provide secure connections to their remote workers and network of office branches, without the bloat of multiple applications.



Social engineering is an evergreen threat that will continue to reach across industry lines and user bases as attackers adopt new technology like deepfakes

Attackers can always count on human fallibility as the one constant amid economies and technologies in flux. It's why social engineering-based attacks will never go out of style — they're versatile enough that we foresee the arrival of souped-up versions of tried-and-tested tactics in 2023. Social attacks are normally centered around current events and issues that have a broad public appeal,[31] but more specifically, we'll see a rise in more complex romance scams. Online fraudsters will continue to be on the prowl for lonely hearts who are more likely to fall for a new spin on the classic honey trap, which involves malicious actors using fake user profiles to lure potential victims into a romantic relationship and trick them out of their money.

The grift has evolved from swindlers who typically feign a plight as a pretext for needing financial aid:[32] the end game for some cons is to phish for a victim's personally identifiable information (PII) on fake dating sites, while more recent ones, like "pig butchering" or Sha Zhu Pan scams, aim to convince victims to invest in fake cryptocurrency trading platforms.[33]

Dating scams are big business, and as of 2022, the US Federal Trade Commission (FTC) reports that this topped the list of fraud categories over the last five years, wresting a whopping US$1.3 billion from its victims.[34] Digital dating fraud only worsened during the pandemic,[35] and until the world's fully in the clear of Covid-19, we can expect cybercriminals to find new ways of preying on unsuspecting victims looking for love during lockdown.

"Online fraudsters will continue to be on the prowl for lonely hearts who are more likely to fall for a new spin on the classic honey trap."

Another area where we'll see scammers retrofitting age-old techniques with modern toolboxes is in business email compromise (BEC), wherein attackers impersonate high-ranking executives over email to defraud a company. This kind of scam will continue to plague enterprises in 2023. The market for BEC is expected to increase at an annual compound rate of 19.4%. Although the use of open-source email security software will have a hand in impeding that growth, BEC remains a lucrative criminal venture: losses resulting from BEC attacks will amount to around US$2.8 billion by 2027.[36] These can be so financially devastating to enterprises that in a recent advisory, the Federal Bureau of investigation (FBI) warns that BEC is a major threat to the global economy.[37]

BEC attempts have matured to the point where fraudsters have added "BEC-as-a-service" to their playbooks,[38] a clear indication that cybercriminals in this space are becoming tech-savvy and professional enough to shop around their skill sets as a new revenue stream. The abundance and accessibility of information online will help attackers further refine their BEC schemes and make them more highly targeted: Poor password hygiene may make credential theft easy and a wealth of log-in details is sold on the dark web,[39] but bad actors have proven that they don't even have to break the law to get a lock on their next target when they can just purchase extensive email lists from legitimate lead-generation businesses that offer such data for marketing purposes.[40]

Malicious actors will continue to tap into the potential of Artificial Intelligence (AI) and machine-learning technologies, using deepfakes to elevate the social engineering side of their BEC attacks — something that we have already observed in the wild in our own research.[41] Deepfakes will have a wide range of use cases for cybercriminals in 2023, enabling them to impersonate victims that can trick banking establishments, cryptocurrency services, or even create user accounts for identity theft. Scams involving deepfakes are uncommon for now, but these have been gaining popularity in underground communities offering services for image and video fakes;[42] it won't be long before the tools and techniques behind such attacks become more widely available to cybercriminals.[43]

The hype surrounding digital novelties like NFTs and the metaverse will keep waning, but the blockchain technology on which they're built is going to be where the real action is

Interest in NFTs and the metaverse, once headline-grabbing internet darlings, will continue to be in freefall[44] in 2023. Early in 2022, the world was in the grip of NFT mania and a staggering $17.2 billion was traded on the NFT market, only for trading volumes to fall to $466.9 million by September.[45] While NFT-related scams may still exist in 2023, these won't leave a significant impact, as we expect that high NFT prices[46] will have dampened the public's enthusiasm for them at this point.

At the height of its popularity, people were buying up NFT avatars and other digital collectibles that were widely believed to eventually become part of metaverse worlds,[47] 3D virtual spaces that the internet had pinned its hopes on as the fertile ground on which innovations in communication and collaboration would thrive.[48] But the metaverse has since fallen short of those expectations, with technology experts now divided as to whether it is truly here to stay.[49] As work on the metaverse continues, we predict that pockets of illegal activity will still take place specifically in the Darkverse,[50] the criminal underbelly of Meta's Metaverse, where bad actors will be drawn together in small underground communities. But ultimately, cybercriminals go where the crowds are, so we anticipate that these will be isolated incidents in 2023.

> **While NFT-related scams may still exist in 2023, these won't leave a significant impact, as we expect that high NFT prices will have dampened the public's enthusiasm for them at this point.**

In sharp contrast, the year ahead will find blockchain a frontier country bustling with activity. We expect to see blockchain in this busy state not only at the onset of 2023, but over the following years, not least of all because it powers the secure and decentralized record of cryptocurrency transactions. Though the buzz surrounding digital currencies has also taken a hit thanks to an abundance of scammers seeking to infiltrate users' crypto-wallets and steal their mnemonic seed phrases,[51] the internet at large won't completely write these off because they will remain useful for users and attackers alike. Cryptocurrencies like Monero, equipped with privacy features that give attackers more freedom to operate with anonymity,[52] will still be widely used by malicious actors for fund transfers. But considering the volatility of digital currencies,[53] we foresee people cashing out to a fiat currency quickly instead of storing funds in their wallets to get ahead of drastic market drops. This change in user behavior will, in turn, motivate malicious actors to carry out more money laundering schemes.

We also predict cryptocurrency-related attacks will keep coming out of countries where attackers have developed a specialty for targeting digital assets. In 2022 alone, specific hacker groups have been eyed as suspects in high-profile heists such as those against a US-based company that facilitates asset transfers over blockchains called Horizon Bridge,[54] and the online game Axie Infinity whose users can earn cryptocurrency while playing.[55] According to a banking report, interest in cryptocurrency stems from the anonymity it provides and the difficulty in tracing transactions[56] that can help secure funding and resources.[57]

More specifically, we foresee cryptocurrency exchanges at increased risk of compromise in the coming year: Attackers will no doubt be attracted to exchanges, for these function much like the banks and brokers of the cryptocurrency world but are not beholden to the same insurance and disclosure regulations as brick-and-mortar financial institutions.[58] More importantly, threat actors stand to gain millions of dollars from targeting these platforms, as demonstrated by attacks on the likes of Liquid Global,[59] FTX,[60] and Binance.[61]

Attackers will further capitalize on vulnerabilities and intrude through overlooked attack surfaces like open-source software

Malicious actors are nothing if not creative, always examining an enterprise's security posture at different angles to find cracks in the armor. Malicious actors in 2023 will be banking on busy companies neglecting to review and replace outdated protocols in their networks — a dangerous oversight that could open the door for cyberattacks: notably, a 2021 survey found that 92% of organizations continued to run unsecure protocols, including Microsoft's SMBv1 protocol. Vendor support have long since been discontinued for these older protocols,[62] which many ransomware variants commonly abuse to infiltrate networks, so enterprises that insist on using them will put themselves at risk of WannaCry and NotPetya ransomware infections.[63]

Overlooked parts of device security, like router use, will also invite unwanted attention from cybercriminals: Attackers that want to go under the radar will likely take advantage of an organization's lack of visibility over devices connected to their corporate networks, especially if these organizations have been negligent in updating the firmware or maintaining activity logs. Even with vendors warning their customers of the dangers that vulnerable routers pose — as was the case with the Cyclops Blink botnet that targeted Asus Wi-Fi routers,[64] for example — a 2022 study suggests that most router users have never considered upgrading their device, giving malicious actors the perfect attack vector in the age of the internet of things (IoT).[65]

Internet-facing devices and more exotic systems will be exposed to further risk brought on by the emergence of malware that's written in uncommon programming languages, like Rust and Golang. These enable cybercriminals to cross-compile their malware to different operating systems, making the next wave of malware variants that much more difficult for defenders to detect, analyze, and reverse-engineer.[66]

In 2023, we also foresee attackers taking a closer look at how software is constructed and focusing their efforts on exploiting vulnerabilities in software's shared components. They're already dialed in on the opportunities in this area, as Sonatype's State of the Software Supply Chain Report found that there was a massive 633% year-on-year spike in malicious attacks on open-source software repositories in 2022, driven by the 3.1 trillion requests worldwide for open-source software.[67] We predict that zero-day vulnerabilities in open-source software will have far-reaching effects for many industries, particularly in the automotive space, where it is widely used in vehicles' chips, hardware, firmware, operating systems, and applications.

Following the discovery of critical flaws in Log4j that made the internet reevaluate its implicit trust in open-source software, we're already starting to the public and private sectors set up defenses against attackers who may take advantage of such vulnerabilities: Google, for instance, has launched a bug bounty program for its open-source software's third-party dependencies in hopes of catching and addressing flaws before they can be weaponized by bad actors.[68] Alongside other tech giants like Apple, Amazon, and IBM, Google has also proposed setting up a group dedicated to the maintenance and support for open-source projects.[69] For their part, legislators in the US are beginning to recognize the important role that open-source software will play in shaping the digital world, as evidenced by the introduction of the Securing Open Source Software Act[70] that, if signed into law, would call on the Cybersecurity and Infrastructure Security Agency (CISA) to work on a risk framework and offer security measures that can guide the US federal government in their use of open-source software.

These days, most software is to some extent made up of third-party code that is either commissioned specifically for a software product or an off-the-shelf, pre-built component designed for a specific function.[71] This could incentivize attackers to infiltrate popular resources like the Python Package Index (PyPI) or the JavaScript package manager npm to pass off their malware as legitimate code. Now that most cloud-native projects are dependent on libraries and dependencies that include open-source software,[72] malware in disguise is a liability that may blindside enterprises: because software libraries are often incorporated during a project's development lifecycle and are rarely scanned for known vulnerabilities in the process, any weaknesses would effectively be baked into a company's cloud-based operations.

Enterprises will need put in the legwork to scan and patch their software configurations periodically, ideally under an airtight vulnerability management plan, to fortify their defenses. Compared to smaller businesses, mature ones are more likely to already have their own open-source software security policy in place, along with teams dedicated to overseeing software security and automated monitoring measures to stave off the supply-chain attacks from malicious actors who want to capitalize on the pervasiveness of open-source software.[73] However, they'll also need to create a software bill of materials (SBOM) for each application they use: A SBOM will become fundamental to how enterprises practice software security and supply chain risk management, functioning much like an inventory of software components and dependencies that lets companies know what software versions and systems are affected as soon as they're made aware of a software security flaw.[74]

Industrial entities will top off their tech stack, but struggle to keep up with staff shortages and vertical regulations

It may be tempting to play it safe in the face of a possible recession, but opportunity costs are lower in times of crisis, freeing up budgets for digital transformation without hurting the bottom line.[75] In the lead up to economic slowdowns that may come in 2023, we foresee mature companies investing in advanced technology such as 5G connectivity. The recent innovations in 5G that enable it to now support enhanced mobile broadband (eMBB), ultra-reliable and low-latency communication (URLLC), and massive machine type communication (mMTC) promises to open up new use cases and market opportunities for enterprises along their industrial internet of things (IIoT) journey.[76]

With contributions from

txOne networks

The growing need among manufacturers for networks with high dependability and low latency is certain to drive up the 5G IIoT market worldwide, which is expected to be worth US$18.9 billion by 2030;[77] any lulls in economic activity will present them with the ideal opportunity to evolve past 4G networks.

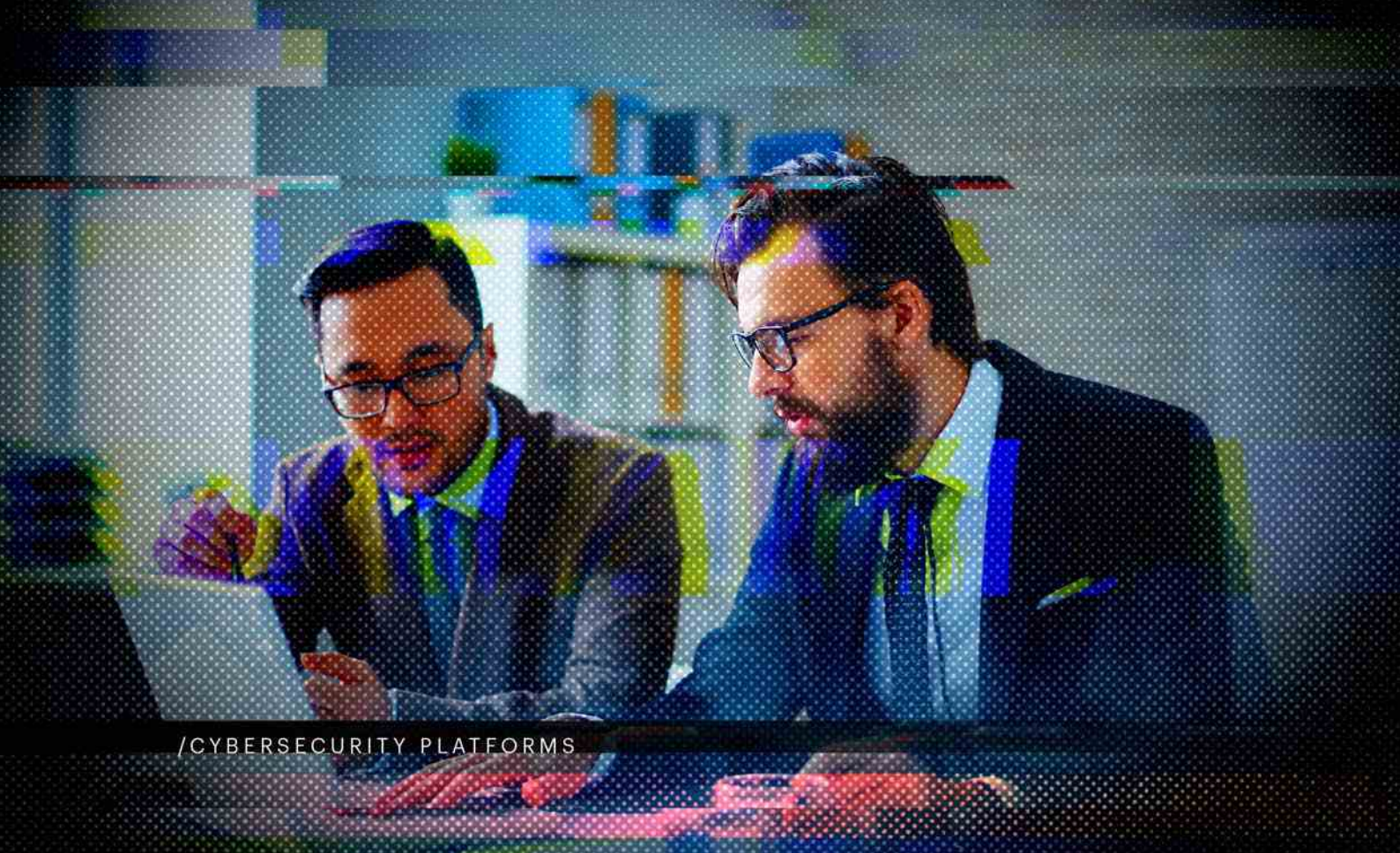
In the lead up to economic slowdowns that may come in 2023, we foresee mature companies investing in advanced technology such as 5G connectivity.

Similarly, we anticipate more original equipment manufacturers (OEM) gradually coming out with offerings and solutions that incorporate AI. Full-scale AI adoption among factories won't happen overnight, but it will be accelerated in select areas of their operations, particularly ones that have very high yield requirements. For companies looking to digitize their plants, AI-powered tools also promise to be a force multiplier of efficiency, enabling them to better predict customers' purchasing behaviors[78] and automate complex tasks for the human operators overseeing their industrial assets.[79] As manufacturers turn to IT to gain a competitive advantage, malicious actors will also capitalize on this emerging technology to ramp up their attacks in terms of automation and probing,[80] making offensive AI a looming threat that should be on manufacturers' radars in the years to come.

The increased integration of IT and OT[81] brought about by these transformative technologies will become a double-edged sword for industrial companies, especially those that keep security strategies for their IT and OT infrastructures separate: while this convergence enables them to monitor their operations closely,[82] it will also expose organizations to unforeseen threats. In 2023, we foresee an upward trend in IT-based cyberattacks inadvertently affecting OT systems that are connected to IT networks – and worse, revealing OT systems as an underutilized attack vector through which malicious actors can move laterally between OT and IT environments.[83]

While companies are covering their bases on this front, the real challenge is finding talent to keep the technology airtight, and operational technology and industrial control systems (OT/ICS) will be among those hit hardest by the security skills gap in 2023. Cybersecurity challenges in this space often involve manpower shortages and human error,[84] which we predict will leave the OT systems of industrial environments limping under understaffed security teams tasked with protecting networks of multiple factories. Threat actors have been known to practice on systems similar to those of an industrial target to develop customized and OT/ICS-focused malware,[85] so manufacturers that can't find qualified personnel to helm the new technologies they've adopted may find themselves at the receiving end of OT/ICS disruptions. Based on our own research, such disruptions can cause financial losses of up to an average of US$2.8 million per incident.[86]

The need for OT/ICS security expertise is also essential in managing the vertical market requirements for cybersecurity,[87] more of which will come to the fore in the year ahead. OT systems are already tightly regulated among certain industries, as is the case for US manufacturers of diagnostic machines[88] and maritime vessels,[89] and we see even more companies taking steps toward collaboration and self-regulation in the year ahead. Modern industrial facilities have been known to be proactive when it comes to protecting their own: Cybersecurity guidelines can be handed down from parent companies or set by upper management, but many smart factories adopt security measures mainly to comply with established industry-wide standards.[90] However, manufacturers will have to stay on top of an uptick in both vertical and government-mandated regulations that aim to create increasingly controlled OT/ICS environments. Although such regulations may exist on the national and federal level, industrial cyberattacks like the ones against Colonial Pipeline's supply chain[91] will have also galvanized lawmakers into preventing future attacks by introducing more cybersecurity-focused directives in the same vein as Executive Order (EO) 14028, or "Improving the Nation's Cybersecurity," in the US.[92]



/CYBERSECURITY PLATFORMS

Enterprises will veer away from the point-solution approach to cybersecurity

In 2023, a slew of enterprises will see the writing on the wall and make the long-overdue shift to more holistic cybersecurity strategies. While many continue to rely on a repertoire of heterogenous, often siloed, point solutions that are designed to address threat issues piecemeal, these disparate tools no longer measure up to the increasingly sophisticated cyberthreats that enterprises must contend with, especially in the cloud-native age. These individual solutions eventually pile up, flooding security teams with daily alerts that put overworked defenders in danger of alert fatigue.[93] On average, organizations deploy 46 individual security monitoring tools, which has them struggling to figure out which alerts to prioritize and puts them at further risk of overlooking a legitimate attack.[94]

n response to this, demand for a unified cybersecurity platform is bound to gain traction among organizations whose needs now call for expanded visibility over their increasing assets that are spread across various environments, networks, and operating systems. Companies will need to be in a position to detect malicious activity on their systems on a larger scale if they are to fend off attacks from malicious actors that are shaping up to be even more methodical and professional: a platform-based approach integrates a cybersecurity vendor's own offerings with third-party tools,[95] which not only streamlines the user experience but provides defenders with enterprise-wide visibility and telemetry across their growing IT infrastructure that they will need to map out their attack surface.[96] The challenge set before organizations in the coming year is not just to consolidate their tool sets to stay vigilant against these threat groups, but also play catch-up with those that are now operating akin to a company themselves: the full extent of the Conti gang's organizational structure, for example, includes a human resource department and salaried employees.[97]

Moreover, we foresee these malicious actors showing an increased interest in managed service providers (MSP) as a threat vector rather than targeting individual organizations. Compromising an MSP's network, which has access to its many clients, would allow cybercriminals to strike at the infrastructure of multiple firms at once and maximize the impact of their attacks.[98] We anticipate that attackers won't just seek to compromise MSPs, but managed security service providers (MSSP) and the tools that they use as well. Weaponizing an MSSP's own toolset against them will allow bad actors to better evade defenders, who will have to sort through the many applications used by both the MSSP and their clients' in-house security team to determine the true source of malicious activity.

Security agencies are already on to criminals who may have MSPs in their crosshairs, with the CISA releasing an advisory warning MSPs and their customers to harden their security posture against cybercriminals — specifically, state-sponsored advanced persistent threat (APT) groups — that may throw global supply chains in peril by taking aim at MSPs to get to their customer networks.[99] CISA and its interagency partners recommend a number of countermeasures, including endpoint detection, network defense monitoring, and application allowlisting. These many mitigation capabilities can be better streamlined under a comprehensive platform solution that can scale up alongside growing organizations.

Though we predict that more businesses will come around to the benefits of security platforms, their widespread adoption still requires buy-in from the upper management. Chief finance officers (CFO) will have more of a hand in steering an organization's purchasing priorities on cybersecurity, alongside CISOs, in 2023. However, this may leave short-sighted companies insufficiently protected if their focus is fixed on costs alone rather than capabilities: A recent survey among CFOs worldwide shows that 87% of respondents were confident in their company's ability to avert cyberattacks, despite 61% of them experiencing at least three security incidents in the last 18 months.[100] A security tool sprawl won't help the fact that, according to an Accenture study, many CFOs already feel overwhelmed by all the responsibilities on their plate.[101] The input and involvement of CFOs is crucial to an organization's security posture, since they will also have to contend with rising cyber insurance premiums and the scrutinizing gaze of insurers who examine a policyholder's existing security measures.[102] Considering this, organizations will have to address this disconnect and awareness gap among their C-suite ranks about the dangers that these cyberthreats pose to their day-to-day operations.

LOOKING AHEAD TO 2023

Trend Micro's predictions for 2023 lays out the trends and risks that will take shape in the cybersecurity landscape, based on the observations and extensive research of our security experts. Getting ahead of the evolving threats that will crop up in the coming year calls for organizations to have a multilayered defense plan, bolstered by mitigation measures such as:

- **Securing environments and systems with a zero trust strategy.** Today's blended work setups would make it reckless for organizations to assume all internal traffic is safe. By adopting the zero trust lens of "never trust, always verify" to their IT architecture, companies can minimize the damage of any future cyberattacks without sacrificing the productivity of users who need access to corporate resources for their work.
- **Investing in user education for employees.** Humans are the last, and weakest, line of defense in cybersecurity — a fact that adversaries won't hesitate to exploit. No amount of safety measures can stop an attacker when your own employees are unwittingly holding the door open for them, so training your workforce to spot security red flags can make all the difference in sidestepping potentially devastating threats.
- **Increasing transparency using a comprehensive security platform.** Enterprises would benefit from consolidating all the monitoring and detection features they need under a single holistic platform. Not only will this improve a company's ability to catch suspicious activity across their networks, but it will also lessen the burden on their security teams and keep defenders sharp. Barring that, companies can whittle their security vendors down to a handful that offer versatile and multifunctional solutions.
- **Unearthing weaknesses in IT infrastructures with a stress test.** Organizations should have a game plan to ensure their readiness in different attack scenarios, especially ones wherein a perimeter gateway has already been breached. For example, enterprises should be able to anticipate how their operations will fare if they had only half the IT manpower to manage the compromise of their internet gateway, domain name system (DNS) records, or any of their critical systems. Allotting time to practicing on simulated attacks gives security teams the hands-on experience, sans the risk.
- **Taking inventory of cloud services to cut down on cloud bloat.** Visibility into the cloud is essential for enterprises if they are to cut through the chaos of managing the many cloud-based services they use. A cloud monitoring strategy should first map out all the solutions that factor into their cloud infrastructure, which will keep security teams informed of what value these services provide to the company, what data these have access to, and who to contact for further support. This will enable them to scrap any redundancies eating up valuable resources and keep pace with growing cloud security compliance standards.

The stark realities of cloud migration, remote working, and software development are sure to test the resilience and readiness of security teams come 2023. To navigate uncertainties that lie ahead in the security landscape, defenders will need a suite of protections capable of assessing and minimizing the risk of compromise on multiple layers. But more importantly, their organization's defense strategy needs to be built on reliable insights into what drives the threat life cycle if they are to come out on top of the cyberthreats arriving in 2023 and beyond.

References

1 Janna Anderson, Lee Rainie, and Emily A. Vogels. (Feb. 18, 2021). *Pew Research Center.* "Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges." Accessed on Nov. 12, 2022, at https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges.

2 Stuart Madnick. (Aug. 29, 2022). *Harvard Business Review.* "New Cybersecurity Regulations Are Coming. Here's How to Prepare." Accessed on Nov. 12, 2022, at https://hbr.org/2022/08/new-cybersecurity-regulations-are-coming-heres-how-to-prepare.

3 The World Bank. (Sept. 15, 2022). *The World Bank.* "Risk of Global Recession in 2023 Rises Amid Simultaneous Rate Hikes." Accessed on Nov. 12, 2022, at https://www.worldbank.org/en/news/press-release/2022/09/15/risk-of-global-recession-in-2023-rises-amid-simultaneous-rate-hikes.

4 Jonathan Greig. (Jan. 13, 2022). *ZDNet.* "After Log4j, White House fears the next big open source vulnerability." Accessed on Nov. 12, 2022, at https://www.zdnet.com/article/after-log4j-white-house-worries-about-the-next-big-open-source-flaw.

5 Jessica Lyons Hardcastle. (June 9, 2022). *The Register.* "Cloud services proving handy for cybercriminals, SANS Institute warns." Accessed on Nov. 20, 2022, at https://www.theregister.com/2022/06/09/criminals_cloud_sans.

6 Zachary Cohen, Kevin Collier, and David Shortell. (Dec. 5, 2019). *CNN.* "US sanctions Russian cybercriminal group 'Evil Corp' over $100 million hack." Accessed on Nov. 18, 2022, at https://edition.cnn.com/2019/12/05/politics/us-sanctions-russian-evil-corp/index.html.

7 Catalin Cimpanu. (Sept. 13, 2019). *ZDNet.* "US Treasury sanctions three North Korean hacking groups." Accessed on Nov. 18, 2022, at https://www.zdnet.com/article/us-treasury-sanctions-three-north-korean-hacking-groups.

8 Danny Palmer. (Jan. 14, 2022). *ZDNet.* "Russian authorities take down REvil ransomware gang." Accessed on Nov. 18, 2022, at https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

9 Matt Burgess. (March 17, 2022). *Wired.* "The Big, Baffling Crypto Dreams of a $180 Million Ransomware Gang." Accessed on Nov. 18, 2022, at https://www.wired.co.uk/article/conti-ransomware-crypto-payments.

10 Ionut Ilascu. (April 15, 2022). *Bleeping Computer.* "Karakurt revealed as data extortion arm of Conti cybercrime syndicate." Accessed on Nov. 18, 2022, at https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate.

11 Mark Haranas. (Nov. 4, 2022). *CRN.* "Gartner: 'Cloud Migration Is Not Stopping' In 2023; $592B Predicted In Public Cloud Spending." Accessed on Nov. 18, 2022, at https://www.crn.com/news/cloud/gartner-cloud-migration-is-not-stopping-in-2023-592b-predicted-in-public-cloud-spending.

12 Josh Stella. (March 18, 2022). *Business Wire.* "Why Ransomware Attacks Steer Clear of the Cloud." Accessed on Nov. 18, 2022, at https://www.businesswire.com/news/home/20220318005081/en/Why-Ransomware-Attacks-Steer-Clear-of-the-Cloud.

13 Jay Chen. (May 16, 2022). *Unit 42.* "A Look Into Public Clouds From the Ransomware Actor's Perspective." Accessed on Nov. 18, 2022, at https://unit42.paloaltonetworks.com/ransomware-in-public-clouds.

14 Robert Lemos. (Aug. 25, 2022). *Dark Reading.* "More Bang for the Buck: Cross-Platform Ransomware Is the Next Problem." Accessed on Nov. 18, 2022, at https://www.darkreading.com/threat-intelligence/cross-platform-ransomware-spikes-problem.

15 Forrester. (Nov. 15, 2022). *Forbes.* "European Predictions For Cloud In 2023." Accessed on Nov. 18, 2022, at https://www.forbes.com/sites/forrester/2022/11/15/european-predictions-for-cloud-in-2023.

16 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Accessed on Nov. 18, 2022, at https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

17 Deep Instinct. (n.d.). *Deep Instinct.* "Living Off The Land Attacks (LOTL)." Accessed on Nov. 18, 2022, at https://www.deepinstinct.com/glossary/living-off-the-land-lotl.

18 Matthew Humphries. (Jan. 13, 2022). *PCMag.* "Teenage Hacker Gains Remote Control of 25 Teslas in 13 Countries." Accessed on Nov. 18, 2022, at https://www.pcmag.com/news/teenage-hacker-gains-remote-control-of-25-teslas-in-13-countries.

19 AT&T Communications. (March 1, 2022). *PRNewswire.* "72% of businesses lack clear hybrid work strategy according to the 2022 Future of Work Study." Accessed on Nov. 18, 2022, at https://www.prnewswire.com/news-releases/72-of-businesses-lack-clear-hybrid-work-strategy-according-to-the-2022-future-of-work-study-301492850.html

20 Cisco. (May 24, 2022). *Cisco.* "Cisco Study: Hybrid work is enhancing employee well-being, but needs to be more inclusive." Accessed on Nov. 18, 2022, at https://news-blogs.cisco.com/apjc/2022/05/24/cisco-study-hybrid-work-is-enhancing-employee-well-being-and-productivity-in-asean-but-efforts-are-needed-to-make-it-more-inclusive.

21 Trend Micro. (Oct. 5, 2022). *Trend Micro Security News.* "Bridging Security Gaps in WFH and Hybrid Setups." Accessed on Nov. 18, 2022, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bridging-security-gaps-in-wfh-and-hybrid-setups.

22 Chris Hockings. (Oct. 22, 2021). *IBM.* "This type of data breach will cost you more time and money." IBM. Accessed on Nov. 18, 2022, at https://www.ibm.com/blogs/ibm-anz/this-type-of-data-breach-will-cost-you-more-time-and-money.

23 Help Net Security. (June 15, 2021). *HelpNet Security.* "VPN attacks up nearly 2000% as companies embrace a hybrid workplace." Accessed on Nov. 18, 2022, at https://www.helpnetsecurity.com/2021/06/15/vpn-attacks-up.

24 Linda Park. (Sept. 26, 2022). *Zscaler.* "2022 VPN Risk Report." Accessed on Nov. 18, 2022, at https://www.zscaler.com/blogs/product-insights/results-are-vpns-are-downright-dangerous.

25 Trend Micro. (n.d.). *Trend Micro.* "What Is Zero trust Networking?" Accessed on Nov. 18, 2022, at https://www.trendmicro.com/en_us/what-is/what-is-zero-trust/zero-trust-networking.html.

26 Mick McCluney and Greg Young. (Jan. 28, 2022). *Trend Micro Research, News, and Perspectives.* "3 Remote Work Security Tips for CISOs." Accessed on Nov. 18, 2022, at https://www.trendmicro.com/en_us/ciso/22/a/remote-work-security-tips.html.

27 Trend Micro. (Aug. 25, 2022). *Trend Micro Research, News, and Perspectives.* "ZTNA vs VPN: Secure Remote Work & Access - SASE Part 2." Accessed on Nov. 18, 2022, at https://www.trendmicro.com/en_us/ciso/22/h/ztna-vs-vpn-secure-remote-work.html.

28 David Holmes and Andre Kindness. (Aug. 2, 2021). *Forrester.* "Introducing The Zero trust Edge Model For Security And Network Services." Accessed on Nov. 18, 2022, at https://www.forrester.com/report/introducing-the-zero-trust-edge-model-for-security-and-network-services/RES161728.

29 Oliver Borchert, Sean Connelly, Scott W. Rose, and Stuart Mitchell. (Aug. 10, 2020). *National Institute of Standards and Technology.* "Zero trust Architecture." Accessed on Nov. 18, 2022, at https://www.nist.gov/publications/zero-trust-architecture.

30 Gartner. (n.d.). *Gartner Glossary.* "Secure Access Service Edge (SASE)." Accessed on November 24, 2022, at https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase.

31 Trend Micro. (n.d.). *Trend Micro.* "Social engineering." Accessed on Nov. 18, 2022, at https://www.trendmicro.com/vinfo/us/security/definition/social-engineering.

32 Trend Micro. (July 19, 2022). *Trend Micro News.* "Top 5 Trending Scams of 2022." Accessed on Nov. 18, 2022, at https://news.trendmicro.com/2022/07/19/top-5-trending-scams-of-2022.

33 Trend Micro. (March 2, 2021). *Trend Micro News.* "Common Romance Scams: Pig Butchering (Sha Zhu Pan), Fake Investment, Sextortion, ... and MORE!" Accessed on Nov. 18, 2022, at https://news.trendmicro.com/2021/03/02/is-it-true-love-things-you-should-know-about-romance-scams.

34 Emma Fletcher. (Feb. 10, 2022). *Federal Trade Commission.* "Reports of romance scams hit record highs in 2021." Accessed on Nov. 18, 2022, at https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021.

35 Claire Ballentine, Misyrlena Egkolfopoulou, and Suzanne Woolley. (June 29, 2022). *Bloomberg.* "Romance Scams Explode, Leaving Broken Hearts and Millions Lost." Accessed on Nov. 18, 2022, at https://www.bloomberg.com/news/articles/2022-06-29/online-fraud-is-soaring-with-tinder-swindler-romance-scams-costing-millions.

36 MarketsandMarkets. (Aug. 15, 2022). *Bloomberg.* "Business Email Compromise (BEC) Market Worth $2.8 Billion By 2027." Accessed on Nov. 18, 2022, at https://www.bloomberg.com/press-releases/2022-08-15/business-email-compromise-bec-market-worth-2-8-billion-by-2027-exclusive-report-by-marketsandmarkets.

37 Federal Bureau of Investigation. (2022). *Federal Bureau of Investigation.* "FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud." Accessed on Nov. 18, 2022, at https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view.

38 Jonathan Greig. (Oct. 21, 2021). *ZDNet.* "Palo Alto warns of BEC-as-a-service, finds average wire fraud attempted is $567,000 with peak of $6 million." Accessed on Nov. 18, 2022, at https://www.zdnet.com/article/palo-alto-warns-of-bec-as-a-service-finds-average-wire-fraud-attempted-is-567000-with-peak-of-6-million.

39 Stu Sjouwerman. (May 18, 2022). *Forbes.* "Beware The Tactics Used For CEO Fraud By BEC Scammers." Accessed on Nov. 18, 2022, at https://www.forbes.com/sites/forbestechcouncil/2022/05/18/beware-the-tactics-used-for-ceo-fraud-by-bec-scammers/?sh=6b617e2d78c7.

40 Kelly Jackson Higgins. (Dec. 04, 2018). *Dark Reading.* "'London Blue' BEC Cybercrime Gang Unmasked." Accessed on Nov. 12, 2022, at https://www.darkreading.com/privacy/-london-blue-bec-cybercrime-gang-unmasked.

41 Craig Gibson, Stephen Hilt, Vladimir Kropotov, and Fyodor Yarochkin. (Sept. 27, 2022). *Trend Micro Research, News, and Perspectives.* "How Underground Groups Use Stolen Identities and Deepfakes." Accessed on Nov. 12, 2022, at https://www.trendmicro.com/en_us/research/22/i/how-underground-groups-use-stolen-identities-and-deepfakes.html.

42 Mayra Rosario Fuentes. (May 26, 2020). *Trend Micro Security News.* "Trading in the Dark: An Investigation into the Current Condition of Underground Markets and Cybercriminal Forums." Accessed on Nov. 18, 2022, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trading-in-the-dark.

43 Michael Hill. (Oct. 25, 2021). *CSO.* "How deepfakes enhance social engineering and authentication threats, and what to do about it." Accessed on Nov. 18, 2022, at https://www.csoonline.com/article/3636992/how-deepfakes-enhance-social-engineering-and-authentication-threats-and-what-to-do-about-it.html.

44 Paul Tassi. (March 10, 2022). *Forbes.* "Interest In NFTs And The Metaverse Is Falling Fast." Accessed on Nov. 18, 2022, at https://www.forbes.com/sites/paultassi/2022/03/10/interest-in-nfts-and-the-metaverse-is-falling-fast/?sh=e03719b1ebbd.

45 Sidhartha Shukla. (Sept. 28, 2022). *Bloomberg.* "NFT Trading Volumes Collapse 97% From January Peak." Accessed on Nov. 18, 2022, at https://www.bloomberg.com/news/articles/2022-09-28/nft-volumes-tumble-97-from-2022-highs-as-frenzy-fades-chart.

46 Kristie Pladson. (Nov. 27, 2021). *Deutsche Welle.* "Why are some NFTs so expensive?" Accessed on Nov. 18, 2022, at https://www.dw.com/en/why-are-some-nonfungible-tokens-so-expensive/a-59921744.

47 Stiven Cartagena. (April 14, 2022). *Entrepreneur.* "The transition from NFTs to the world of the metaverse." Accessed on Nov. 18, 2022, at https://www.entrepreneur.com/business-news/the-transition-from-nfts-to-the-world-of-the-metaverse/424824.

48 Janna Anderson and Lee Rainie. (June 30, 2022). *Pew Research Center.* "The metaverse will fully emerge as its advocates predict." Accessed on Nov. 18, 2022, at https://www.pewresearch.org/internet/2022/06/30/the-metaverse-will-fully-emerge-as-its-advocates-predict.

49 Janna Anderson and Le Rainie. (June 30, 2022). *Pew Research Center.* "The Metaverse in 2040." Accessed on Nov. 12, 2022, at https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040.

50 Trend Micro. (Aug. 8, 2022). *Trend Micro Security News.* "Metaworse? The Trouble with the Metaverse." Accessed on Nov. 12, 2022, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/metaworse-the-trouble-with-the-metaverse.

51 Cifer Fang, Vladimir Kropotov, Loseway Lu, Qi Sun, and Fyodor Yarochkin. (March 24, 2022). *Trend Micro Research, News, and Perspectives.* "An Investigation of Cryptocurrency Scams and Schemes." Accessed on Nov. 18, 2022, at https://www.trendmicro.com/en_us/research/22/c/an-investigation-of-cryptocurrency-scams-and-schemes.html.

52 MacKenzie Sigalos. (June 13, 2021). *CNBC*. "Why some cyber criminals are ditching bitcoin for a cryptocurrency called monero." Accessed on Nov. 18, 2022, at https://www.cnbc.com/2021/06/13/what-is-monero-new-cryptocurrency-of-choice-for-cyber-criminals.html.

53 Omid Malekan. (July 6, 2022). *Harvard Business Review*. "What Skeptics Get Wrong About Crypto's Volatility." Accessed on Nov. 18, 2022, at https://hbr.org/2022/07/what-skeptics-get-wrong-about-cryptos-volatility.

54 The Guardian. (June 30, 2022). *The Guardian*. "North Korean hackers thought to be behind $100m cryptocurrency heist." Accessed on Nov. 18, 2022, at https://www.theguardian.com/world/2022/jun/30/north-korean-hackers-thought-to-be-behind-100m-cryptocurrency-heist.

55 British Broadcasting Corporation. (April 15, 2022). *British Broadcasting Corporation*. "North Korean hackers target gamers in $615m crypto heist - US." Accessed on Nov. 18, 2022, at https://www.bbc.com/news/world-asia-61036733.

56 The Korea Times. (Aug. 27, 2018). *The Korea Times*. "North Korea 'developing bitcoin exchange, mining cryptocurrencies'." Accessed on Nov. 18, 2022, at https://www.koreatimes.co.kr/www/nation/2022/05/103_254535.html.

57 Kim Yoo-chul. (Aug. 31, 2018). *The Korea Times*. "Cryptocurrency: A new revenue source for North Korea?" Accessed on Nov. 18, 2022, at https://www.koreatimes.co.kr/www/nation/2021/05/356_254646.html.

58 Dalton Bennett and Peter Whoriskey. (Nov. 16, 2022). *The Washington Post*. "Crypto's free-wheeling firms lured millions. FTX revealed the dangers." Accessed on Nov. 18, 2022, at https://www.washingtonpost.com/business/2022/11/16/ftx-collapse-crypto-exchanges-regulation.

59 Ian Allison. (Aug 20, 2021). *CoinDesk*. "Liquid Exchange Attack: Can a Crypto Wallet Ever Be 100% Safe From Hacks?" Accessed on Nov. 18, 2022, at https://www.coindesk.com/tech/2021/08/20/liquid-exchange-attack-can-a-crypto-wallet-ever-be-100-safe-from-hacks.

60 Nikhilesh De, Reilly Decker, Sam Kessler, Cheyenne Ligon, and Sam Reynolds. (Nov. 12, 2022). *Yahoo! Finance*. "'FTX Has Been Hacked': Crypto Disaster Worsens as Exchange Sees Mysterious Outflows Exceeding $600M." Accessed on Nov. 18, 2022, at https://finance.yahoo.com/news/ftx-crypto-wallets-see-mysterious-042044681.html.

61 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Accessed on Nov. 18, 2022, at https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

62 Kelsey Milligan. (March 4, 2022). *ExtraHop*. "Why Humility Is What's Needed for CISO Success." Accessed on Nov. 12, 2022, at https://www.extrahop.com/company/blog/2022/ciso-cyber-confidence.

63 Mark Bowling. (March 14, 2022). *ExtraHop*. "Practical Steps for Responding to the CISA Warning on Russian Cyber Attacks." Accessed on Nov. 12, 2022, at https://www.extrahop.com/company/blog/2022/practical-steps-for-responding-to-the-cisa-warning-on-russian-cyberattacks.

64 Michael Crider. (March 21, 2022). *PCWorld*. "Update your Asus router's firmware right now or risk botnet infection." Accessed on Nov. 12, 2022, at https://www.pcworld.com/article/624825/update-your-asus-wi-fi-routers-firmware-right-away.html.

65 Kaspersky. (June 08, 2022). *Kaspersky*. "87 critical vulnerabilities discovered in routers in 2021." Accessed on Nov. 19, 2022, at https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021.

66 Cyware. (Nov. 19, 2021). *Cyware*. "The Rising Popularity of Golang-based Malware." Accessed on November 23, 2022, at https://cyware.com/news/the-rising-popularity-of-golang-based-malware-87b9e7d7.

67 Sonatype. (2022). *Sonatype*. "State of the Software Supply Chain." Accessed on Nov. 18, 2022, at https://www.sonatype.com/state-of-the-software-supply-chain/introduction.

68 Sergiu Gatlan. (Aug. 30, 2022). *Bleeping Computer*. "Google launches open-source software bug bounty program." Accessed on Nov. 18, 2022, at https://www.bleepingcomputer.com/news/google/google-launches-open-source-software-bug-bounty-program.

69 Jonathan Greig. (Jan. 13, 2022). *ZDNet*. "Log4j: Google and IBM call for list of critical open source projects." Accessed on Nov. 12, 2022, at https://www.zdnet.com/article/log4j-after-white-house-meeting-google-calls-for-list-of-critical-open-source-projects.

70 Steven Vaughan-Nichols. (Sept. 29, 2022). *ZDNet*. "What the Securing Open Source Software Act does and what it misses." Accessed on Nov. 18, 2022, at https://www.zdnet.com/article/whats-what-in-the-united-states-securing-open-source-software-act.

71 Curtis Yanko. (Oct. 26, 2022). *Dark Reading*. "Open Source Is Just the Tip of the Iceberg in Software Supply Chain Security." Accessed on Nov. 18, 2022, at https://www.darkreading.com/risk/open-source-is-just-the-tip-of-the-iceberg-in-software-supply-chain-security.

72 Magno Logan. (Oct. 08, 2021). *Trend Micro Security News*. "Minding the Gaps: The State of Vulnerabilities in Cloud Native Applications." Accessed on Nov. 18, 2022, at https://www.trendmicro.com/vinfo/ph/security/news/virtualization-and-cloud/minding-the-gaps-the-state-of-vulnerabilities-in-cloud-native-applications.

73 Robert Lemos. (June 21, 2022). *Dark Reading*. "Open Source Software Security Begins to Mature." Accessed on Nov. 18, 2022, at https://www.darkreading.com/application-security/open-source-software-security-mature.

74 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Accessed on Nov. 18, 2022, at https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

75 Walter Frick. (May-June 2019). *Harvard Business Review*. "How to Survive a Recession and Thrive Afterward." Accessed on Nov. 23, 2022, at https://hbr.org/2019/05/how-to-survive-a-recession-and-thrive-afterward.

76 Jun Morimoto. (July 11, 2022). *Trend Micro Research, News, and Perspectives*. "Private 5G Network Security Expectations Part 3." Accessed on Nov. 23, 2022, at https://www.trendmicro.com/en_ph/research/22/g/private-5g-network-security-part-3.html.

77 PRNewswire. (Sept. 13, 2022). *Dark Reading*. "Global 5G Industrial IoT Market Forecasted To Gain USD 18.9 Billion by 2030, With A Tremendous CAGR of 28% | Growth Market Reports." Accessed on Nov. 25, 2022, at https://www.darkreading.com/prnewswire2.asp?rkey=20220913IO71181&filter=3896.

78 Trend Micro, United Nations Interregional Crime and Justice Research Institute, and Europol. (Nov. 19, 2020). *Trend Micro Security News*. "Exploiting AI: How Cybercriminals Misuse and Abuse AI and ML." Accessed on Nov. 30, 2022, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml.

79 Eleftherios Charalambous, Robert Feldmann, Gérard Richter, and Christoph Schmitz. (March 7, 2019). *McKinsey & Company.* "AI in production: A game changer for manufacturers with heavy assets." Accessed on Nov. 30, 2022, at https://www.mckinsey.com/capabilities/quantumblack/our-insights/ai-in-production-a-game-changer-for-manufacturers-with-heavy-assets.

80 Sharon Goldman. (May 16, 2022). *VentureBeat.* "Crippling AI cyberattacks are inevitable: 4 ways companies can prepare." Accessed on Nov. 30, 2022 at https://venturebeat.com/ai/crippling-ai-cyberattacks-are-inevitable-4-ways-companies-can-prepare.

81 Trend Micro. (March 18, 2020). *Trend Micro Security News.* "The IIoT Threat Landscape: Securing Connected Industries." Accessed on Nov. 30, 2022 at https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/the-iiot-threat-landscape-securing-connected-industries.

82 CIO & Leader. (July 9, 2019). *CIO & Leader.* "IT-Based Attacks Increasingly Impacting OT Systems: Study." Accessed on Nov. 30, 2022, at https://www.cioandleader.com/article/2019/07/09/it-based-attacks-increasingly-impacting-ot-systems-study.

83 TripWire. (May 19, 2021). *TripWire.* "IT Network Attacks Can Impact Your OT Networks, Too." Accessed on Nov. 30, 2022, at https://www.tripwire.com/state-of-security/it-network-attacks-can-impact-your-ot-networks-too.

84 Eduard Kovacs. (July 14, 2022). *SecurityWeek.* "Two Big OT Security Concerns Related to People: Human Error and Staff Shortages." Accessed on Nov. 23, 2022, at https://www.securityweek.com/two-big-ot-security-concerns-related-people-human-error-and-staff-shortages.

85 Michael Hill. (Sept. 26, 2022). *CSO Online.* "US CISA/NSA release new OT/ICS security guidance, reveal 5 steps threat actors take to compromise assets." Accessed on Nov. 23, 2022, at https://www.csoonline.com/article/3674832/us-cisa-nsa-release-new-ot-ics-security-guidance-reveal-5-steps-threat-actors-take-to-compromise-as.html.

86 Trend Micro. (June 2, 2022). *Trend Micro News.* "Cyber-Attacks on Industrial Assets Cost Firms Millions." Accessed on Nov. 23, 2022, at https://newsroom.trendmicro.com/2022-06-02-Cyber-Attacks-on-Industrial-Assets-Cost-Firms-Millions.

87 Kaspersky. (May 17, 2022). *Kaspersky.* "OT security team shortage threatens protection in every fifth industrial organization." Accessed on Nov. 25, 2022, at https://www.kaspersky.com/about/press-releases/2022_ot-security-team-shortage-threatens-protection-in-every-fifth-industrial-organization.

88 ZScaler. (n.d.). *ZScaler.* "What Is Operational Technology (OT) Security?" Accessed on Nov. 25, 2022, at https://www.zscaler.com/resources/security-terms-glossary/what-is-operational-technology-ot-security.

89 Ryan Moody. (June 13, 2022). *Forbes.* "Cooperation—Not Regulations—Will Protect Our Critical Infrastructure." Accessed on Nov. 25, 2022, at https://www.forbes.com/sites/forbestechcouncil/2022/06/13/cooperation-not-regulations-will-protect-our-critical-infrastructure/?sh=3f0fa14b4abe.

90 Trend Micro. (April 12, 2021). *Trend Micro Research, News, and Perspectives.* "Survey 3 Standard is way to institute collaboration." Accessed on Nov. 25, 2022, at https://www.trendmicro.com/en_ph/research/21/d/new-survey-report-released-the-state-of-industrial-cybersecurity-part-3.html.

91 Derek B. Johnson. (May 9, 2022). *SC Magazine.* "US proposes $1 million fine for Colonial Pipeline ransomware attack." Accessed on Nov. 25, 2022, at https://www.scmagazine.com/analysis/critical-infrastructure/us-proposes-1-million-fine-for-colonial-pipeline-ransomware-attack.

92 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives.* "An In-Depth Look at ICS Vulnerabilities Part 1." Accessed on Nov. 25, 2022, at https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

93 Bharat Mistry. (May 2021). *Trend Micro.* "Why SecOps analysts are struggling to keep their heads above water." Accessed on Nov. 18, 2022, at https://resources.trendmicro.com/rs/945-CXD-062/images/TMVO-opinion-Why_SecOps_analysts_are_struggling-May2021.pdf.

94 Trend Micro. (Oct. 12, 2021). *Trend Micro.* "Cybersecurity Tool Sprawl Drives Plans to Outsource Detection and Response." Accessed on Nov. 18, 2022, at https://www.multivu.com/players/English/8967351-trend-micro-cybersecurity-tool-sprawl-drives-plans-outsource-detection-response.

95 Trend Micro. (June 13, 2022). *Trend Micro CISO Resource Center.* "Addressing Cyber Risk with a Unified Platform." Accessed on November 23, 2022, at https://www.trendmicro.com/en_us/ciso/22/f/addressing-cyber-risk-with-a-unified-platform.html.

96 Jon Clay. (Oct. 11, 2022). *Trend Micro Research, News, and Perspectives.* "Enhance Cyber Defense with 2022 Cybersecurity Trends." Accessed on November 23, 2022, at https://www.trendmicro.com/en_us/ciso/22/j/cybersecurity-trends-2022-cyber-defense.html.

97 Monica Pitrelli. (April 13, 2022). *CNBC.* "Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'." Accessed on Nov. 18, 2022, at https://www.cnbc.com/2022/04/14/conti-ransomware-leak-shows-group-operates-like-normal-tech-company.html.

98 Nikolay Pankov. (March 27, 2019). *Kaspersky.* "MSPs as a threat vector." Accessed on Nov. 18, 2022, at https://www.kaspersky.com/blog/msp-as-a-threat-vector/26209.

99 Cybersecurity & Infrastructure Security Agency. (May 11, 2022). *Cybersecurity & Infrastructure Security Agency.* "CISA, NSA, FBI and International Cyber Authorities Issue Cybersecurity Advisory to Protect Managed Service Providers (MSP) and Customers." Accessed on Nov. 18, 2022, at https://www.cisa.gov/news/2022/05/11/joint-cybersecurity-advisory-protect-msp-providers-and-customers.

100 James McLeary, Greg Michaels, and William Rimington. (Sept. 13, 2022). *Kroll.* "Cyber Risk and CFOs: Over-Confidence is Costly." Accessed on Nov. 18, 2022, at https://www.kroll.com/en/insights/publications/cyber/cyber-risk-and-cfos.

101 Michela Coppola, Jason Dess, Aneel Delawalla, and Cherene Powell. (Oct. 19, 2022). *Accenture.* "How CFOs can turn any decision dilemma into growth." Accessed on Nov. 18, 2022, at https://www.accenture.com/us-en/insights/consulting/cfo-decision-paradox-success-paradigm.

102 Jim DeLoach. (June 21, 2022). *Forbes.* "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Accessed on November 23, 2022, at https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

FUTURE/TENSE

TREND MICRO
SECURITY PREDICTIONS
FOR 2023

TREND MICRO | research

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com