Progress® Flowmon®

The Cybersecurity Outlook for 2023

REPORT

The Cybersecurity Outlook for 2023

Global cyber-attacks have gone up by 81 percent since the onset of the pandemic as both public and private enterprises are struggling to maintain a strong security posture against continuously increasing and evolving cyber threats. This uptick in cyber-attacks is due in large part to the heightened reliance on the internet for a myriad of services and functions during the pandemic, as well as a shift to working from home (WFH) instead of traditional office environments. These two factors greatly expand the attack surface for potential hackers.

The tectonic shift to remote work as well, as online retail and business purchasing, has made cybersecurity risks a critical concern for both consumers and organizations. Businesses and consumers alike are now coming to terms with the implications of living and transacting in an increasingly digitized world where multi-factor authentication (MFA) and virtual private networks (VPN) have become the new norms for secure access. Unfortunately, hackers are still managing to stay ahead of the curve and eluding even the most well-protected enterprises and even government organizations.

Despite the dreary outlook, several notable trends and patterns can be anticipated for 2023 and beyond. Aside from the continued increase in cyber-attacks across the globe, enterprises are learning to engage with cyber threats on a different level, focusing on managing cyber risk instead of the futile task of eliminating threats in their entirety. Just as driving an automobile inherently presents certain risks to drivers and passengers, connecting the business to the internet makes cyber risk exposure unavoidable. The following white paper provides an overview of the cybersecurity landscape for 2023 and how organizations are maneuvering to manage their cyber risk more effectively in the face of rising threats.

Cloud Adoption and Expansion

The adoption of cloud offerings and cloud-based infrastructure platforms has exploded in the past several years, primarily in the form of infrastructure as a service (IaaS), software as a service (SaaS) and managed cloud services and hybrid cloud solutions. According to Gartner, global spending on public cloud services is anticipated to hit $600 billion in 2023. This dramatic uptick in cloud adoption has resulted in a significant attack surface expansion and an increase of targets for malicious actors to compromise.

Third-Party Risk

In today's highly globalized and interconnected economies, more and more businesses rely on a series of third-party integrations to deliver products or features in a unified manner to the end user. Supply chains are as intricate as they are risky, and some of the most devastating cyber-attacks to date, including the infamous 2013 Target Data Hack and the recent SolarWinds hack, were the result of supply chain security breakdowns. Enterprises should not only closely monitor their security posture, but also that of their partners and suppliers.

In other words, you're only as strong as your weakest link — considering today's highly integrated value chains, this mantra has never been more true. The consequences of a third-party cybersecurity failure are shared across the value chain, even if organizations downstream are not directly at fault. Third-party risk includes both negative impacts on organizations' operating environments, compliance, and legal risk exposure (e.g., GDPR, HIPAA, SOC2), as well as brand damage and tarnished current/future customer trust.

Cybersecurity Talent Shortages

As the number of cyber-attacks continues to increase year over year, organizations are hard-pressed to both retain existing security professionals and hire new talent. This deficit of professional resources continues to pose challenges for organizations looking to bolster their human defenses against would-be hackers. An estimated 3.5 million unfilled cybersecurity jobs are expected to flood the market by 2025; suffice to say, good cybersecurity talent will still be hard to come by in 2023 and beyond.

The drivers behind the current cyber talent shortage are multi-faceted and varied—however, most causes originate from the relatively recent wave of digital transformations sweeping up industries across the board. Naturally, this has resulted in a dearth of qualified security professionals; firms are also struggling to upskill their current staff to meet rising security challenges and vacancies resulting from the diversification/specialization of security roles.

Though this shortage in cybersecurity talent is a crucial pain point shared by the majority of organizations, business firms need to mitigate cyber risk with the limited staff on hand through the right tools and technologies. Businesses and entities that are proactively planning, applying the right tools and equipping their current team members with the skills for success are the ones that will be best positioned to mitigate or eliminate cyber threats.

Continued Low Detection Rates & Pressing Geopolitical Concerns

According to the World Economic Forum's 2020 Global Risk Report, the cyber attack detection rate in the U.S. that year was an astonishingly low 0.05 percent. Because the vast majority of breaches are left undetected, organizations are now cognizant of the need for better security technologies and, perhaps more importantly, skilled cybersecurity professionals to manage and interpret the data/analytics generated by those technologies.

As mentioned previously, the current cybersecurity talent shortage makes the latter highly challenging for the foreseeable future. The best-protected enterprises will therefore be capable of assuming a vigilant posture that combines the use of automated monitoring tools with the heightened detection/response capabilities of security specialists.

This combination of technology and tools has grown even more critical in the last few months as geopolitical impacts invariably cross over into the cyber domain. World events have further complicated the threat landscape, with Russia's invasion of Ukraine acting as a further catalyst for cyber warfare.

Currently, the most critical shared concern of the U.S. and EU is KillNet, a pro-Russian group responsible for continued distributed denial of service (DDoS) attacks against pro-NATO countries and organizations.

If history is any indication, the mantra "together, we are stronger" will again prove itself as the only sustainable, rational maneuver forward in this increasingly hyper-connected world. This fact is certainly manifest in recent geo-political events—conflicts poised to create new alliances and bolster/re-affirm existing pacts, as well as trigger heightened activity on the cybersecurity front. In terms of both geo-political and cyber conflicts, collective security for companies will prove to be the safest path forward in today's hostile threat landscape (cyber and otherwise) in 2023 and beyond.

Cost of Cyber Breaches

The sharp increase in cyber attacks during the pandemic illustrates that, above all else, cyber attackers are relentless and undaunted opportunists, even as the world grapples with the ongoing pandemic and health crisis. Five hundred seventy-six businesses in the United States of America were compromised by ransomware in 2021. Since then, the cost of ransomware attacks has been steadily on the rise, with losses anticipated to top $30 billion globally by 2023.

Malicious actors carrying out today and tomorrow's ransomware campaigns are looking to sabotage critical network infrastructure entry points via exposures in cloud services — while, of course, continuing to rely on unpatched software and social engineering as their tried-and-true method. This is especially vexing for large organizations that lack comprehensive visibility and awareness into their environments—for example, the National Health Services, which is still battling to contain a two-month-old ransomware outbreak and rein in its compromised IT assets.

Data Security, Compliance & Regulatory Trends

Despite the growing sophistication of cyber-attacks, business firms have at least some responsibility in reducing the impact radius of cyber incidents, both through better preventative controls and post-breach activities. All the aforementioned drivers have resulted in more cyber-attacks, and governments and regulatory bodies are reacting swiftly—both to attackers as well as to their potentially negligent targets.

A myriad of new rules/regulations and standards are being developed by the U.S. Federal Trade Commission, Food and Drug Administration, Department of Transportation, Department of Energy and, of course, the Cybersecurity and Infrastructure Security Agency. Similarly, the White House, Congress, Securities and Exchange Commission (SEC) and other local agencies and governments are focusing on rules for reporting cyber incidents. On the state level, 36 U.S. states enacted new cybersecurity-related legislation in 2021. And across the globe, both China and Russia have instituted new data localization measures, while countries like India and the EU have expanded or added additional detail levels to their incident reporting requirements.

Conclusion

If history is any indication, third-party cyber in 2023 risk will continue to dominate the risk landscape as firms become increasingly connected through integrated software supply chains and vendor relationships. To reduce their attack surface and mitigate potential security exposures, organizations need to consider the impact that third parties, partners, vendors and even customers have on their overall cyber risk posture.

From a compliance perspective, laws and regulations will likely get more stringent in 2023 and beyond. In terms of talent, highly trained security professionals will continue to be coveted by organizations large and small across all industries. The organizations that continue to be creative with the resources, tools and employees they currently have on hand can effectively enable their security staff to do more with less.

From DevOps to data science and cybersecurity, most IT disciplines deploy network traffic monitoring extensively to gain visibility and situational awareness. Proper infrastructure and network traffic monitoring, as well as anomaly detection and response, are critical for maintaining continuity and continuous improvement in modern organizations' IT environments. Flowmon can enable your network and security teams to achieve their shared goal – a stable and healthy digital environment. As networks are becoming more complex, hybrid environments more common and threats ever more elusive, Flowmon is the key to ensuring that your business can operate safely, with greater agility and without being susceptible to modern threats. For more information on how your organization can benefit from deep infrastructure awareness and visibility, please visit the Flowmon website or try it out for 30-days for free.

Request your FREE trial of Flowmon for 30-days

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to build the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com

f /progresssw
/progresssw
/progresssw
in /progress-software
/progress_sw_

Progress®